TECHNICAL CODE

BUSINESS CONTINUITY MANAGEMENT - REQUIREMENTS (FIRST REVISION)

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date: 8 August 2024

MCMC MTSFB TC G014:2024

Development of technical codes

The Communications and Multimedia Act 1998 ('the Act') provides for Technical Standards Forum designated under Section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to Section 185 of the Act shall consist of, at least, the requirement for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with Section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by Section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under Section 185 of the Act.

A technical code prepared in accordance with Section 185 shall not be effective until it is registered by the Commission pursuant to Section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8688 8000
Fax : +60 3 8688 1000
Email : stpd@mcmc.gov.my
Website: www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Level 3A, MCMC Tower 2
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8680 9950
Fax : +60 3 8680 9940
Email : support@mtsfb.org.my
Website: www.mtsfb.org.my

Contents

Committee representation

This technical code was developed by Fundamental Security Technologies Sub Working Group which supervised by Security, Trust and Privacy Working Group under the Malaysian Technical Standards Forum Bhd (MTSFB) which consists of representatives from the following organisations:

Deloitte Business Advisory Sdn Bhd

Digiforen (M) Sdn Bhd

Digital Nasional Berhad

FNS (M) Sdn Bhd

Maxis Broadband Sdn Bhd

TM Technologies Services Sdn Bhd

U Mobile Sdn Bhd

Universiti Kuala Lumpur

Foreword

This technical code for Business Continuity Management - Requirements (First Revision) ('this Technical Code') was developed pursuant to Section 185 of Act 588 by the Malaysian Technical Standards Forum Bhd (MTSFB) via its Fundamental Security Technologies Sub Working Group.

Major modifications in this revision are as follows:

a) Update the relevant clauses to align with ISO 22301:2019, *Security and resilience - Business continuity management systems - Requirements.*

b) Remove clause 8.2 on incident response personnel and clause 10.2 on evaluation of business continuity procedures.

c) Include Annex B on business impact analysis and risk assessment guidelines.

This Technical Code replaces the MCMC MTSFB TC G014:2018, *Business Continuity Management (BCM) - Requirements.* The latter shall be deemed to be invalid to the extent of any conflict with this Technical Code.

Information marked as "NOTE" is for guidance in understanding or clarifying the associated requirement.

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

BUSINESS CONTINUITY MANAGEMENT (BCM) - REQUIREMENTS

0. Introduction

The implementation of Business Continuity Management (BCM) within organisations facilitates the systematic identification and mitigation of potential disruptions.

The BCM implementation is expected to provide the following benefits:

a) Enhances organisational resilience, ensuring that core functions and services can endure adverse circumstances.

b) Assists in fulfilling legal and regulatory obligations, thus averting potential fines and penalties.

c) Safeguards an organisation's reputation and cultivates trust among stakeholders and clientele.

d) Drives operational efficiency, cost savings, and process improvements while guaranteeing the continuity of vital operations during crises.

e) Aids in securing favourable insurance coverage terms and premiums, offering a competitive edge and reinforcing supply chain resilience.

f) Prioritises employee safety and well-being, underpins financial stability, and fosters peace of mind for leadership, employees, and stakeholders alike.

g) Serves as an essential investment in the long-term viability and prosperity of organisations.

Business continuity is the capability of the organisation to continue the delivery of products or services at acceptable predefined capacities following a disruption. BCM is the process of implementing and maintaining business continuity in order to prevent loss and prepare for, mitigate and manage disruptions.

Disruptions have the potential to interrupt the organisation’s entire operations and its ability to deliver products and services. However, implementing a BCM before a disruption occurs, rather than responding in an unplanned manner after the incident, will enable the organisation to resume operations before unacceptable levels of impact arise.

The organisation’s approach to business continuity management and its documented information should be appropriate to its context (e.g., operating environment, complexity, needs, resources).

Activities can be disrupted by a wide variety of incidents, many of which are difficult to predict or analyse. By focusing on the impact of disruption rather than the cause, business continuity enables an organisation to identify activities that are essential to it being able to meet its obligations. Through business continuity, an organisation can recognise what is to be done to protect its resources (e.g., people, premises, technology, information), supply chain, interested parties and reputation before a disruption occurs. With that recognition, the organisation can put in place a response structure, so that it can be confident of managing the impacts of a disruption.

Business continuity can be effective in dealing with both sudden disruptions (e.g., explosions) and gradual ones (e.g., pandemics). Figure 1 and Figure 2 illustrate conceptually how business continuity can be effective in mitigating impacts in certain situations. No particular timescales are implied by the relative distance between the stages depicted in either diagram.

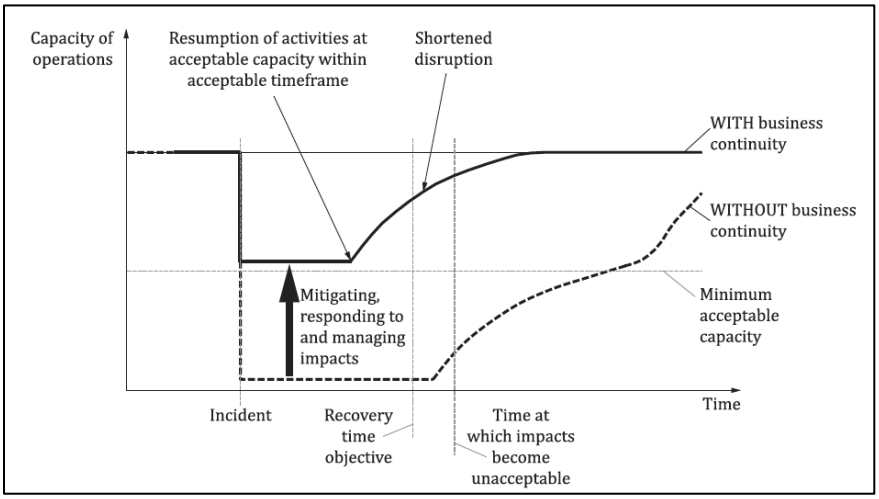

Figure 1. Illustration of business continuity being effective for sudden disruption

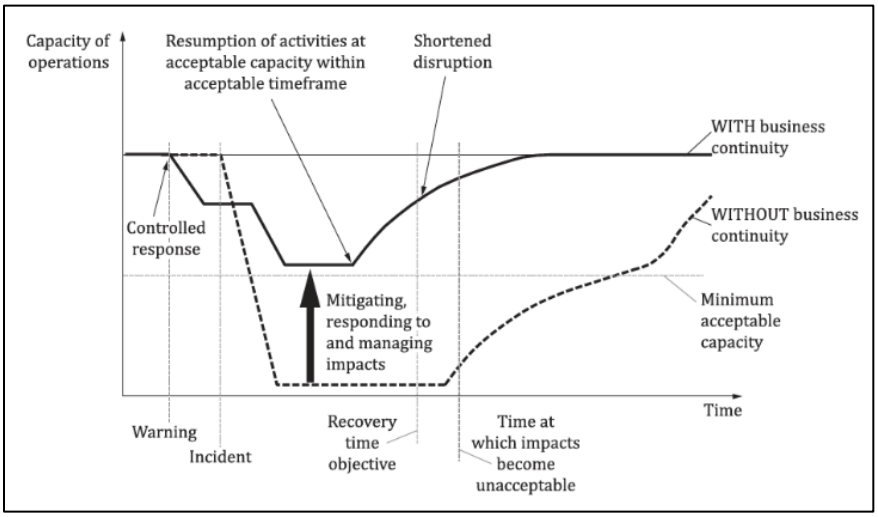

Figure 2. Illustration of business continuity being effective for gradual disruption

1. Scope

This Technical Code defines the requirements that support the implementation of the BCM in an organisation. The requirement set out in this Technical Code are generic and intended to be applicable to any size of organisation.

2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For updated references, the latest edition of the normative references (including any amendments) applies.

ISO 22301, *Security and resilience - Business continuity management systems - Requirements*

ISO 22313, *Security and resilience - Business continuity management systems - Guidance on the use of ISO 22301*

ISO/IEC 27031, *Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity*

ISO/IEC 22361, Security and resilience - Crisis Management - Guidelines

ISO 31000, *Risk management - Principles and guidelines*

3. Abbreviations

For the purpose of this Technical Code, the following abbreviations apply.

BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
DRII	Disaster Recovery Institute International
ICT	Information and Communications Technology
IRBC	ICT Readiness for Business Continuity
IT	Information Technology
MAO	Maximum Acceptable Outage
MBCO	Minimum Business Continuity Objective
MTD	Maximum Tolerable Downtime
MTPD	Maximum Tolerable Period of Disruption
RA	Risk Assessment
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement

4. Terms and definitions

For the purposes of this Technical Code, the following terms and definitions apply.

4.1 Business continuity

Capability of an organisation to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption.

4.2 Business Continuity Management (BCM)

Holistic management process of implementing and maintaining the capability of an organisation to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption.

4.3 Business Continuity Plan (BCP)

Documented information that guides an organisation to respond to disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives.

4.4 Business Impact Analysis (BIA)

Process of analysing the impact over time of disruption on the organisation.

NOTES:

1. The outcome is a statement and justification of business continuity requirements.

2. Disaster Recovery Institute International (DRII) defines Business Impact Analysis (BIA) as a method of identifying the effects of failing to perform a function or requirement.

4.5 Capacity

Combination of all the strengths and resources available within an organisation, community or society that can reduce the level of risk or the effects of a crisis.

NOTE: Capacity can include physical, institutional, social, or economic means as well as skilled personnel or attributes such as leadership and management.

4.6 Crisis

Unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property or the environment.

4.7 Critical business functions

Vital functions without which an organisation will either not survive or will lose the capability to effectively achieve its critical objectives, such as delivery of key products and services, operational support functions etc.

4.8 Disaster

Situation where widespread human, material, economic or environmental losses have occurred that exceeded the ability of the affected organisation, community or society to respond and recover using its own resources.

4.9 Disruption

Incident, whether anticipated or unanticipated, that cause an unplanned, negative deviation from the expected delivery of products and services according to an organisation’s objectives.

4.10 Emergency

Sudden, urgent, usually unexpected occurrences or event requiring immediate action.

NOTE: An emergency is usually a disruption or condition that can often be anticipated or prepared for, but seldom exactly foreseen.

4.11 Facility

Plant, machinery, property, building, transportation units at sea/land/airport, and other items of infrastructure or plant and related systems that have a distinct and quantifiable business function of service.

NOTE: A facility can have formal boundaries as defined by, for example, legislation.

4.12 Interested party

Person or organisation that can affect, be affected by or perceive themselves to be affected by a decision or activity, i.e. customers, owners, personnel, providers, bankers, regulators, unions, partners, or society that can include competitors or opposing pressure groups.

NOTES:

1. A decision maker can be an interested party.

2. Impacted communities and local populations are considered to be interested parties.

4.13 Maximum Tolerable Period of Disruption (MTPD)

Time it would take for adverse impacts, which can arise as a result of not providing a product or service or performing an activity, to become unacceptable.

NOTE: Some standards or best practice documents use Maximum Tolerable Downtime (MTD) or Maximum Acceptable Outage (MAO).

4.14 Minimum Business Continuity Objective (MBCO)

Minimum capacity or level of services and/or products that is acceptable to an organisation to achieve its business objectives during a disruption.

4.15 Product and service

Output or outcome provided by an organisation to interested parties, i.e. manufactured items, internet services, cloud services.

4.16 Recovery

Restoration and improvement, where appropriate, of operations, facilities, livelihoods or living conditions of affected organisations, including efforts to reduce risk factors.

4.17 Recovery Point Objective (RPO)

Point to which information used by an activity is restored to enable the activity to operate on resumption.

NOTE: Can also be referred to as maximum data loss.

4.18 Recovery strategies

An approach by an organisation that will ensure its recovery and continuity in the face of disruptions. Plans and methodologies are determined by the organisation’s strategy. There is more than one solution to fulfil an organisation’s strategy (e.g., internal or external hot site, or cold site, alternate work area reciprocal agreement, mobile recovery).

NOTE: Some standards or best practices use satellite site.

4.19 Recovery Time Objective (RTO)

Period of time following an incident within which a product and service or an activity is resumed, or resources are recovered.

NOTES:

1. For product, services and activities, the Recovery Time Objective (RTO) is the time goal for the restoration

and recovery of functions or resources based on the acceptable down time and acceptable level of performance in case of a disruption of operations.

2. The acceptable level may vary based on the legal and regulatory requirements and Business Continuity Objective defined by the organisation.

4.20 Risk Assessment (RA)

Overall process of risk identification, risk analysis and risk evaluation. It involves the process of identifying internal and external threats and vulnerabilities, identifying the likelihood and impact of an event arising from such threats or vulnerabilities, defining critical functions necessary to continue the organisation's operations, defining the controls in place necessary to reduce exposure, and evaluating the cost of such controls.

NOTES:

1. Risk assessment is described in detail in ISO 31000:2018.

2. DRII defines RA as the process of identifying the risks to an organisation, assessing the critical functions necessary for an organisation to continue business operations, defining the controls in place to reduce organisation exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.

4.21 Top management

Person or group of people who directs and controls an organisation at the highest level.

NOTES:

1. Top management has the power to delegate authority and provide resources within the organisation.

2. If the scope of the BCM covers only part of an organisation, then top management refers to those who direct and control that part of the organisation.

5. Context of organisation

5.1 Understanding the organisation and its context

The organisation shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its BCM.

NOTE: These issues will be influenced by the organisation's overall objectives, its products and services and the amount and type of risk that it may or may not take.

5.2 Understanding the needs and expectations of interested parties

The organisation shall determine the interested parties and requirements of the interested parties that are relevant to the BCM against disruptive events, crises, and emergencies.

The organisation shall implement and maintain a process to identify, provide access to, and assess the applicable legal and regulatory requirements related to the continuity of its products and services, activities, and resources.

NOTE: The legal and regulatory requirements may be mandated by the regulatory bodies or stated on a Service Legal Agreement (SLA) that the organisation has agreed to the clients. This information shall be documented and keep up to date.

5.3 Scope of Business Continuity Management (BCM)

The scope shall enable the organisation to determine the boundaries and applicability of the BCM. The organisation shall establish BCM capabilities and competencies which will enable it to continue, recover and resume critical business functions to meet these requirements.

When determining the BCM scope, the organisation shall consider the expectations from the interested parties and the regulatory requirements in 5.2.

The organisation shall perform the following:

a) Establish the parts of the organisation to be included in the BCM, taking into account its location(s), size, nature and complexity.

b) Identify products and services to be included in the BCM.

NOTE: Part of the organisation may be a department or division within the organisation. The organisation should consider a particular end-to-end function.

5.4 Exclusion

When defining the scope, the organisation shall document and explain exclusions. They shall not affect the organisation's ability and responsibility to provide business continuity, as determined by the business impact analysis or risk assessment and applicable legal or regulatory requirements.

6. Leadership

Leadership is essential to ensure the BCM is relevant and applicable to the organisation. Strategic decisions and directions will guide the team to develop and implement a BCM that meets the objectives. Good leadership will provide assurance that essential resources and budget to support the agreed recovery strategies.

Top management is responsible for ensuring the development, implementation, maintenance, and effectiveness of the BCM in the organisation.

A business continuity manager, with the appropriate level of responsibilities, competencies, and authority, shall be appointed to lead the team implementing or maintaining the BCM and provide guidance.

6.1 Management commitment

Top management shall provide evidence of its commitment to the development and implementation of the BCM and continually improve its effectiveness by the following:

a) Complying with applicable legal, regulatory and other requirements to which the organisation subscribes.

b) Integrating BCM processes into the organisation's established maintenance and review procedures.

c) Establishing business continuity policy and objectives in line with the organisation's objectives, obligations and strategic direction.

d) Appointing one or more persons with the appropriate authority and competencies to be responsible for the BCM and accountable for its effective operation.

e) Ensuring that BCM roles, responsibilities and competencies are established.

f) Ensuring the availability of sufficient resources, including a monetary support.

g) Communicating to the organisation the importance of fulfilling business continuity policy and objectives.

h) Ensuring that internal BCM audits are conducted.

i) Ensuring regular management reviews of the BCM.

j) Directing and supporting the improvement of the BCM.

k) Operational involvement through steering groups.

l) Inclusion of business continuity as an item at management meetings.

6.2 Policy

Top management is responsible for steering BCM with policies and strategies necessary for the continuation of critical business functions by providing a framework for setting business continuity objectives. In addition, the business continuity policy shall demonstrate sufficient awareness of the risks, mitigating measures and state of readiness by way of confirmation to the organisation.

The top management shall establish a business continuity policy that consists of the following:

a) Appropriate to the purpose of the organisation.

b) Provides a framework for setting business continuity objectives.

c) Includes a commitment to satisfy applicable requirements.

d) Includes a commitment to continual improvement of BCM.

The BCM policy shall be available in documented information and being communicated within the organisation as well as available to the interested party, as appropriate.

6.3 Organisational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organisation.

Top management shall assign the responsibilities and authority for the following:

a) Ensuring that the BCM conforms to the requirements of this technical code.

b) Reporting on the performance of the BCM to the top management.

NOTE: For organisation that has sufficient resources, it may establish a dedicated BCM steering committee which consists of relevant top management. The BCM working committee that is led by the Business Continuity Manager, who is responsible for supporting and reporting the performance of the BCM to the steering committee.

The working committee shall comprise BCM coordinators who represent the relevant division or department to ensure the business continuity meets the objectives of the BCM steering committee, which includes business units defined from the BIA process.

The organisation shall retain documented information that defines the roles and responsibilities of individuals and/or committees responsible for BCM.

7. Planning

7.1 Addressing risks and opportunities

When planning for the BCM, the organisation shall consider the issues referred to the context of organisation and determine the risks and opportunities that need to be addressed as follows:

a) Ensure the management system can achieve its intended outcome(s).

b) Prevent, or reduce, undesired effects.

c) Achieve continual improvement.

The organisation shall plan the following:

a) Action to address these risks and opportunities.

b) How to integrate and implement the actions into its BCM processes.

c) How to evaluate the effectiveness of these actions.

NOTE: In the due course of performing any evaluation, the party performing the evaluation should be at minimal independent from the implementor. Evaluator shall have the sufficient knowledge and competency when acting as evaluator.

7.2 Business continuity objectives and plans to achieve them

Top management shall ensure that business continuity objectives are established and communicated for relevant and levels within the organisation.

The business continuity objectives shall determine the following:

a) Be consistent with the business continuity policy.

b) The organisation’s business functions that require contingency measures.

c) Take account of the minimum acceptable level of organisation objectives.

d) Be measurable.

e) Take into account applicable requirements.

f) Be monitored and updated as appropriate.

To achieve its business continuity objectives, the organisation shall determine the following.

a) Roles and responsibilities.

b) What will be done.

c) Resources required.

d) When it will be completed.

e) How the results will be measured and evaluated.

The organisation shall retain documented information on the business continuity objectives.

8. Support

The organisation shall determine and provide the resources needed for the BCM as follows:

a) Achieve its business continuity policy and objectives.

b) Meet the changing requirements of the organisation.

c) Enable effective communication on business continuity management matters, internally and externally.

d) Provide for the ongoing operation and continual improvement of the business continuity management.

These shall be provided in a timely and efficient manner.

8.1 Business Continuity Management (BCM) resources

When identifying the resources required for the BCM, the organisation shall make adequate provision for the following:

a) People and people-related resources, include the following:

   i) The time necessary to fulfil BCM roles and responsibilities.

   ii) Training, education, awareness and exercising.

   iii) Management of BCM personnel.

b) Facilities, including appropriate work locations and infrastructure.

c) Information and Communications Technology (ICT), including applications and security controls that support effective and efficient programme management.

d) Management and control of all forms of documented information.

e) Communication with the interested party.

f) Finance and funding.

Resources and their allocation shall be reviewed periodically in order to ensure their adequacy.

8.2 Competence

The organisation shall establish an appropriate and effective system for managing the competence of persons undertaking BCM work under its control.

Management shall determine the competencies required for all BCM roles and responsibilities and the awareness, knowledge, understanding, skills and experience needed to fulfil them. All assigned personnel with BCM roles within the organisation shall demonstrate the competencies required and be provided with training, education, development and other support needed to do so.

The organisation shall identify and deliver the business continuity functional training requirements of

relevant participants and evaluate the effectiveness of its delivery.

Response skills and competence throughout the organisation shall be developed by practical training, including active participation in exercises.

The organisation shall establish training and awareness programmes for employees that shall be affected by a disruptive incident.

8.3 Awareness

Persons doing work under the business continuity management shall be aware of the following:

a) The business continuity policy.

b) Their contribution to the effectiveness of the BCM, including the benefits of improved business continuity management performance.

c) The implications of not conforming to the BCM requirements.

d) Their own role and responsibility during disruptive incidents.

Top management shall progressively promote an organisational culture that places a high priority on enhancing business continuity capability and ensures BCM becomes an integral part of the strategic management process and routine business operations. Awareness and periodic briefings for the top management are equally important to ensure continuing commitment and support for the BCM.

8.4 Communication

Communication plans shall be established to address the needs based on the criticality of business disruptions. It should be established for escalation during disruption, during crisis, during execution of business communication plans etc.

NOTE: Communication plans should be established for escalation during disruption, during crisis, during execution of business communication plans etc.

When establishing the communication plan, it shall include the following:

a) On what it will communicate

The organisation shall consider the legal or regulatory obligations to communicate. Communication regarding the BCM can be needed depending on the nature of the organisation and situation.

b) When communication should take place

There can be thresholds beyond which it becomes imperative for the organisation to communicate, and the organisation’s context can dictate how frequently communication should take place.

c) With whom it will communicate

All interested parties will require communication from time to time, so it is important to determine the circumstances in which communication will be needed and the communication priorities for each interested party.

d) The means of communication

Determining in advance the methods, tools and channels of communication, including alternatives, will enable the organisation to communicate effectively.

e) The persons to execute the communication

The organisation shall maintain an emergency contact list of all relevant parties and key recovery personnel essential for the swift response and recovery of critical business functions. The contact list shall be regularly updated.

The organisation should identify spokespersons to represent the organisation and designate specific people to be points of contact for communication.

8.5 Document control and change management

The organisation shall maintain the documented information required by this Technical Code as evidence of conformity to the requirements and effective operation of the BCM.

The organisation shall ensure that access to the documents and information related to BCM are granted based on as needed basis and only to its authorised personnel.

Any amendment to BCM documentation and BCP shall undergo a formal change management process to ensure the changes are approved by appropriate and authorised management level.

The organisation shall maintain the external documents and the BCM implementation records to ensure the effectiveness of the BCM.

9. Operations

9.1 Operational planning and control

The organisation shall determine, plan, implement and control those actions needed to fulfil its business continuity policy and objectives and meet applicable needs and requirements.

These actions shall be combined to create a programme to ensure that the organisation’s business continuity is managed appropriately and its effectiveness maintained.

The organisation shall establish control mechanisms within the programme that include the following:

a) Deciding how these actions shall be determined, planned, implemented and controlled, for example by establishing an implementation plan and agreeing on a suitable methodology for implementing BCP.

b) Ensuring that controls over these actions are implemented in accordance with the decisions made by, for example, setting project milestones and specifying required deliverables.

c) Keeping documented information to demonstrate that the processes have been carried out as planned.

The organisation shall ensure that planned changes are controlled, unintended changes are reviewed, and appropriate action is taken. Figure 3 illustrates the elements of operational planning and control.

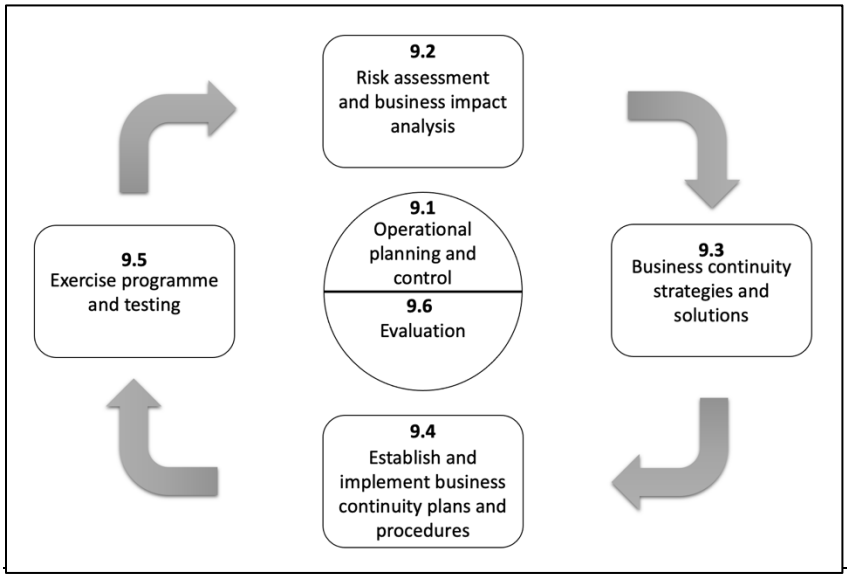

Figure 3. Elements of BCM operational planning and control

9.2 Risk assessment (RA) and Business Impact Analysis (BIA)

9.2.1 Risk Assessment (RA)

The organisation shall ensure that each business area determines its critical resources and processes. The organisation shall identify and assess potential threats that could severely interrupt operations and business activities through structured Risk Assessment (RA) process. For business-critical processes, the impact of a complete or partial failure of the corresponding resources is measured by means of an impact analysis.

The risk assessment shall be carried out at least annually or more frequently if there are significant changes to the internal operations or external environments.

The organisation shall measure the likelihood of the identified threats occurring and determine the impact on the organisation. The organisation is expected to carry out a BIA annually which forms the foundation for developing the BCP and whenever there are material changes to the organisation's business activities.

9.2.2 Business Impact Analysis (BIA)

The organisation shall establish, implement, and maintain a formal and documented BIA that evaluates and determines continuity and recovery priorities, objectives and targets.

The BIA exercise shall be conducted for all business functions within the scope (as in 5.2) in a structured and systematic manner, so as to identify critical business functions, resources and infrastructure of the organisation.

This assessment shall consider mutual interdependencies between business areas (upstream or downstream processes) and dependencies in connection with the interested party.

The analysis is intended to indicate.

a) The desired extent to which business-critical processes are to be recovered.

b) The maximum period until the recovery of business-critical processes.

c) The impacts that a disruption of these activities would have on the organisation.

d) The minimum scope of resources or replacement (buildings, staff, IT or data centre, physical security, external providers) that shall be available in the event of a crisis in order to achieve the desired level of recovery.

e) Interdependencies and dependencies between business areas and/or interested parties.

9.2.2.1 Maximum Tolerable Period of Disruption (MTPD) and Recovery Time Objective (RTO)

The organisation shall determine the thresholds of impact that are unacceptable to the organisation. The time it would take for impacts to become unacceptable can be referred to as the "maximum tolerable period of disruption (MTPD)", "maximum tolerable period", or "maximum acceptable outage". The minimum level of product or service that is acceptable to the organisation can be expressed as the "minimum business continuity objective (MBCO)". The goal is to develop a BCP that details the procedures and the minimum level of resources required to recover the critical business functions within the recovery timeframe and maintain services at an acceptable level.

The organisation shall also set the time frame for resuming an activity to achieve the MBCO, referred to as the activity's "recovery time objective (RTO)" by taking dependencies on the related activities and the complexity of the recovery process. It may be appropriate for organisations with complex recovery processes to set multiple RTOs for a range of acceptable capacities.

The MBCO, MTPD and RTO shall correspond with the importance and criticality of the business functions. The organisation shall establish BCO and RTO for business functions that have a significant impact and shall not exceed MTPD. All MBCOs, Recovery Point Objectives (RPOs) and RTOs of critical business functions shall be validated and approved by top management.

The organisation shall consider incorporating specific RTO requirements in contractual arrangements with an interested party.

NOTE: The determination of MTPD shall be undertaken and guided by Top Management or the relevant committee.

9.2.2.2 Recovery Point Objective (RPO)

The organisation shall determine the RPO for each critical business function in order to develop the backup strategy that enables the business function activity to operate on recovery.

The RPO shall be validated and approved by top management or the relevant committee.

Figure 4 illustrates the relationship between RPO, RTO, MBCO and MTPD.

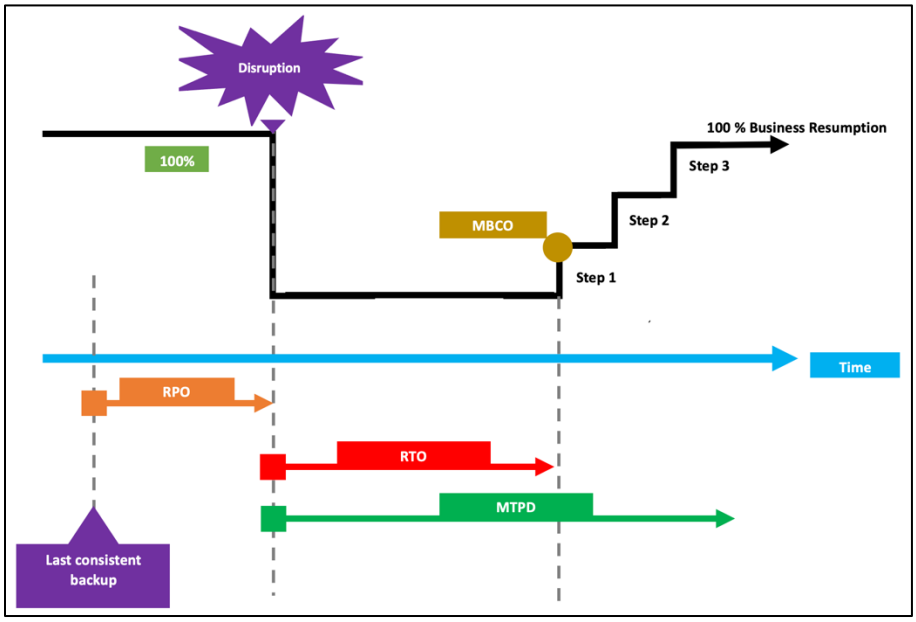

Figure 4. RPO, RTO, MBCO and MTPD concept

Table 1 describes the RPO, RTO, MBCO and MTPD.

Table 1. Description of RPO, RTO, MBCO and MTPD

Concept	Explanation
RTO	Recovery Time Objective: Refers to the maximum acceptable length of time that can elapse before the lack of a business function severely impacts the organisation.
RPO	Recovery Point Objective: Refers to much data an organisation can afford to lose during a disruption.
MBCO	Minimum Business Continuity Objectives: Refer to the minimum level of services and/or products that is acceptable to the organisation to achieve the organisation's business objectives when disruption happened.
MTPD	Maximum Tolerable Period of Disruption: Refer to the maximum allowable time that the organisation's key products or services is made unavailable or cannot be delivered before its impact is deemed as unacceptable.

Table A.1 of Annex A shall be used as a sample of qualitative measurement in prioritising the organisation's key functions and services.

9.2.2.3 Crisis management

A crisis is an inherently abnormal, unstable and complex situation that represents a threat to the strategic objectives, reputation or existence of an organisation. It is an event that can, within a short period of time, harm the organisation's constituents, its facility, its finances or its reputation.

The organisation should establish coordinated activities to lead, direct, and control an organisation with regard to a crisis and it should align with the organisation's crisis management procedures.

NOTE: For details of implementation on crisis management, please refer to the relevant international standards

ISO/IEC 22361, *Security and resilience - Crisis Management - Guidelines*.

9.3 Business continuity strategies and solutions

The organisation shall formulate and document appropriate business continuity strategy for all critical business functions to ensure the continuity or recovery of essential services within the acceptable timeframe.

Business continuity strategy lays down the fundamental procedure with which the company intends to achieve the recovery objectives for the underlying scenarios and their impact on resources identified in the BIA and RA.

The organisation shall also consider proactive and reactive measures that control the risks as follows:

a) Reduce the likelihood of disruption.

b) Shorten the period of disruption.

c) Limit the impact of disruption on the organisation’s critical business functions.

The recovery strategies are part of business continuity strategies that shall indicate the following:

a) The recovery timeframe.

b) Delivery of the minimum level of essential services.

c) Functional relocation.

d) The alternate and recovery sites.

e) Resources such as key personnel including the decision makers, work area, data, facility and technology requirements, where appropriate.

The continuity strategies shall be:

a) Documented and approved by management or relevant committees to ensure alignment with corporate goals and business objectives.

b) Regularly reviewed to ensure relevancy as business activities and operating environment change.

9.4 Establish and implement business continuity plan & procedures

The organisation shall put in place documented procedures that provide overall control of the response to a disruptive incident and resume activities within their RTO.

a) Specific

Immediate steps that shall be taken during a disruption.

b) Flexible

Ability to respond to unanticipated threat scenarios and changing internal and external conditions.

c) Focused

Clearly related to the impact of events that could potentially disrupt operations and be developed based on stated assumptions and analysis of interdependencies.

d) Effective

Minimising the consequences of incidents through the implementation of appropriate mitigation strategies.

NOTE: Once the documented plan and procedures are in place, the appropriate internal and external communications protocol should be executed to ensure both Organisation's staffs and Stakeholders are made aware of the changes in place. Affected parties are require ensuring that the changes are being assess using Risk Management approach to understand the potential gap and determine if remediation is necessary.

9.4.1 Business Continuity Plans (BCPs)

The organisation shall develop a workable BCP for all critical business functions.

Management shall be involved in business continuity planning. The responsibility of management in ensuring that a well-designed plan is developed does not diminish although the BCP formulation is undertaken by a competent BCM practitioner.

The BCP shall include, at least.

a) Procedures to be followed in response to a major disruption to business operations. The procedures shall enable the organisation to respond swiftly to a crisis situation, recover and resume the critical business functions, resources and infrastructure outlined in the BCP within the stipulated timeframe.

b) Escalation, declaration and notification procedures. The organisations shall maintain a call tree and contact list.

c) The conditions for BCP activation and the individual with authority to declare a disaster and grant permission to execute the recovery processes.

d) A list of all resources required to recover critical business functions in the face of a major disruption. This shall include but not limited to, key recovery personnel, computer hardware and software, office equipment, facilities and relevant documentation.

e) Relevant information about the alternate and recovery sites.

f) Procedures for restoring normal business operations. This shall include the orderly entry of all business transactions and records into the relevant IT systems and the completion of all verification and reconciliation procedures.

The organisation shall ensure that their BCPs have adequate arrangements and resources to deal with a possible emergence of a pandemic or infectious disease. The organisation is encouraged to align their preparatory and response measures to the outbreak stages used by the relevant government authority.

The organisation shall ensure that recovery personnel's responsibilities are clearly documented in the BCP. During a major disruption, staff could be unavailable for various reasons, hence alternate recovery personnel be identified for all critical business functions.

9.4.2 Alternate and recovery sites

The organisation shall make available a functional alternate and recovery site in the event the business premises, key infrastructure and systems supporting critical business functions become unavailable.

The alternate and recovery sites shall either be in house arrangements, or available through an agreement with interested party recovery facility provider, or a combination of both options.

The organisation shall assess the suitability and capacity of the alternate and/or recovery site to ensure that the site is.

a) Sufficiently distanced from the primary site to avoid being affected by the same disaster or source of disruption.

b) Using a separate or alternative telecommunication network and power grid from the primary site to avoid a 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.

d) For technology requirements, the organisation shall ensure that the systems at the recovery sites are:

   i) Compatible with the organisation's primary systems (in terms of capacity and capability as agreed to RTO, RPO, MTPD and BCO) to adequately support the critical business functions.

   ii) Continuously updated with a current version of systems and application software to reflect any changes to the organisation's system configurations (e.g., hardware or software upgrades or modifications).

The organisation shall provide a recovery facility (hot site, online mirroring, etc), which commensurate with its established RTO/RPO/MTPD/BCO and for critical business functions.

For the use of an interested party alternate site or recovery facility, the organisation shall perform the following.

a) Establish a written contract to safeguard the organisation's interest.

b) Provide a Service Level Agreement (SLA) between the organisation and the interested party to determine the level and type of services to be provided to the organisation. The SLA shall be properly documented and approved by the management.

c) Assess the capacity and capability of the interested party sites for a reasonably prolonged period.

d) Ensure that adequate physical and logical access control is provided by the interested party to safeguard the recovery facility.

The organisation shall ensure that a periodic and continuous review and monitoring be undertaken on the service level provided by the interested party and the measures mentioned in items b), c) and d) above.

The organisation shall ensure that the backup strategy is consistent with the agreed RPO of respective business functions.

NOTE: The evaluation of alternate and recovery sites should be based on Risk Assessment methodology to ensure factors such as likelihood and impact are taken in consideration.

9.4.3 Critical business information records

The organisation shall ensure that a sufficient number of backup copies of critical business information, software and related hardcopy documentation (for systems and users) are available for the recovery of critical business functions. A copy of the information, documentation and software shall be made available at an offsite premise or backup site, and any changes or updates shall be done periodically and reflected in all copies.

A full systems backup shall be periodically conducted and shall at least consist of the updated version

of the operating system software, production programs, system utilities and all master and transaction files. The frequency of backup would depend on its criticality and shall be performed after critical modification or updates. All backup media shall be:

a) Properly labelled using standard naming conventions that at least indicate usage, date and retention schedules.

b) Regularly tested to ensure that it can be restored when necessary.

c) Rotated in a systematic and timely cycle.

d) Stored offsite in a secure and access-controlled environment, which is of the consistent standard to the main site and in accordance with manufacturer's recommendations.

e) Located at a distance that would protect it from damage resulting from an incident at the primary site but facilitates quick retrieval process.

f) The transportation to the backup site done in a controlled and secured manner with proper authorisation and record.

g) Disposed of using established procedures.

9.5 Exercising programme and testing

The organisation shall exercise and test with business continuity procedures to ensure consistency with the organisational business continuity objective.

a) Regular

Organisations may carry out different types of tests. Taking into consideration the criticality of the business functions, the complexities, resources required and the testing objectives, organisations shall conduct tests in modules and at different but regular intervals. Management and staff shall participate in these exercises and be familiar with their roles and responsibilities in the event of activation.

b) Complete and meaningful

All components of a business process should be meaningfully tested (e.g., from frontline through to supporting and processing components, etc.). This shall include testing the connectivity, functionality and load capacity of the infrastructure provided at the recovery site(s). Organisations should satisfy themselves that their exercise programmes adequately cover both the qualitative (e.g., response time, etc.) and quantitative (e.g., volume capacity, etc.) aspects.

They shall critically challenge all strategic and planning assumptions regularly to ascertain their applicability, especially when the business scope or direction changes. Completeness would also include the awareness and preparedness of staff and coordination with external parties, as well as thorough testing of all interdependencies.

Organisations shall progressively make their exercises more challenging and introduce different scenarios each time they conduct the same type of exercise. This would lead to an increase in confidence in their business continuity preparedness.

Exercises shall include a combination any of the following.

a) Desktop walk through.

b) Simple/partial system test to a full system test.

c) Staff call-tree activation (with and without mobilisation).

d) Alternative arrangements of shared services.

e) Backup disk restoration.

f) Retrieval of vital records.

NOTE: The above options serve as a guideline, Organisation shall determine through Risk Assessment the suitable exercise scenario combination to implemented. Various factors to be taken into consideration include but not limited to Organisation regulatory and legal requirement, maturity to undertake the increasing complicate exercise, availability of resources and skillset.

Formal exercise documentation and debrief, postmortem reviews listing lessons learnt and any new risk mitigating measures shall be prepared. Management representative or management shall sign-off on the documentation and concur with the proposed new mitigating measures.

Minimum BCP testing requirements shall include, but not limited to the following:

a) Verifying completeness of the plan and adequacy of recovery procedures.

b) Assessing familiarity of staff with their business continuity responsibilities and the organisation's evacuation procedures.

c) Evaluating connectivity, functionality, performance and load capacity of alternate and recovery sites.

d) Assessing the adequacy of security implementation and staff awareness.

e) Assessing the effectiveness of communication plan and coordination with relevant parties.

f) Evaluating response time.

g) Recommending remedial actions for future tests.

BCP test results for critical business function and application shall be timely communicated to the top management.

9.6 Evaluation of business continuity documentation and capabilities

The organisation shall evaluate the business continuity documentation and capabilities as follows:

a) Perform appropriate appropriateness, completeness and effectiveness of the relevant elements of the business continuity plan covering business impact analysis, risk assessment, strategies, solutions, plans and procedures.

b) Perform assessment against business continuity plan by way of reviews, analysis, exercises, tests, post-incident reports and performance evaluations.

c) Perform assessment of business continuity effectiveness with affected business partners and supply chain supplier.

d) Assess the business continuity plan conformity to the relevant national law, regulatory industry requirement, industry best practices, and conformity with organisation own business continuity policy and objectives.

e) Ensure documentation is up to date to reflect the procedures in update documentation and

procedures in a prompt manner.

These evaluations shall be conducted at planned intervals minimally at least annually, after an incident or activation, and when significant changes occur.

Annex B provides the business impact analysis and risk assessment guidelines.

10. Performance evaluation

10.1 Monitoring, measurement, analysis and evaluation

The procedures for the performance and the effectiveness of the BCM shall include the following.

a) The setting of performance metrics.

b) Assessment of the protection of prioritised activities.

c) Confirmation of compliance with requirements.

d) Examination of historical evidence.

e) Use of documented information to facilitate subsequent corrective actions.

The procedures for monitoring performance shall include the following:

a) The setting of performance metrics including qualitative and quantitative measurements that are appropriate to the needs of the organisation.

b) Monitoring the extent to which the organisation's business continuity policy and objectives are met.

c) Identifying when the monitoring and measuring should take place.

d) Assessing the performance of the processes, procedures and functions that protect prioritised activities.

e) Proactive measures of performance that monitor compliance of the BCM with applicable legislation, statutory and regulatory requirements.

f) Recording data and results of monitoring and measurement sufficient to facilitate subsequent corrective action analysis.

Procedures shall also make reference to business continuity policy and objectives.

The organisation shall be able to demonstrate that it has identified, evaluated and complied with the legal and regulatory requirements and any other subscribed requirements.

Records of all periodic evaluations and their results shall be maintained. The organisation shall analyse, and at planned intervals, evaluate the outcomes from the monitoring and measurement.

10.2 Internal audit

Internal auditors shall periodically verify that effective BCM practices are implemented in the organisation, in line with the principles and requirements stipulated in this Technical Code and the organisation's BCM policies and procedures.

The organisation shall plan, establish, implement and maintain an audit programme(s) including the

frequency, methods, responsibilities, planning requirements and reporting, which shall take into consideration the importance of the processes concerned and the results of previous audits.

Audit criteria shall be defined in each audit in the planned audit programme.

Auditors' requirements for each audit shall be planned to ensure the competence of auditors to meet the objectives and impartiality of the audit process.

Internal auditors shall review the level of commitment to BCM and overall preparedness against the organisation's BCM policies and regulatory requirements. For outsourced services, the auditors or other independent party shall periodically review the BCP testing undertaken by the outsourcing vendor to ensure their business continuity preparedness. Gaps identified shall be documented in the audit report together with action plans for further improvement by the respective business functions or outsourcing vendor. The audit report shall be submitted to the relevant management.

10.3 Management review

Top management shall review the organisation's BCM, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

Management review shall include an appraisal of the following:

a) The status of actions from previous reviews.

b) The performance of the BCM including trends apparent from non-conformities and corrective actions, the results of monitoring and measurement, and audit findings.

c) Changes to the organisation and its context that might impact the organisation's BCM.

d) Opportunities for continual improvement.

Personnel who are involved in implementing the BCM and allocating its resources shall be involved in the management review.

The output of the management review shall include the result in improvements to the efficiency and performance of the BCM and shall result in the following changes.

a) Variations in the scope.

b) Improvements in its effectiveness.

c) Updates to business continuity procedures.

d) Changes to controls and how their effectiveness is measured.

The organisation shall retain documented information as evidence of the results of management reviews and shall include the following.

a) Communicate the results of management review to the relevant interested party.

b) Take appropriate action relating to those results.

11. Improvement

11.1 Non-conformity and corrective action

The organisation shall do the following to address the non-conformity and in making a corrective action.

a) Identify non-conformities, take action to control, contain and correct them, deal with their disruptions and evaluate the need for action to eliminate their causes.

b) Establish effective procedures to ensure that non-fulfilment of a requirement. The procedure shall cover the following.

   i) Enable ongoing detection, analysis and elimination of actual and potential causes of non-conformities.

   ii) Define responsibilities, authority and steps to be taken in planning and carrying out the corrective action.

c) Planning approach and weaknesses associated with the BCM are identified and communicated in a timely manner to prevent further occurrence of the situation.

d) Identify and address root causes.

e) Management shall ensure that corrective actions are implemented and that there is a systematic follow up to evaluate their effectiveness.

11.2 Continual improvement

The organisation shall continually improve to take the BCM to a higher level of effectiveness by monitoring and reviewing the organisation’s BCM activities.

Annex A
(informative)

Sample of qualitative measurement

Sample of qualitative measurement in prioritising the organisation's key functions and services as shown in Table A.1.

Table A.1. Prioritisation of the organisation's key functions and services

Impact ratings	Impact category	Disruptions description
1 (Minor)	Operation	Little or no disruption to service.
	Reputation	Little or no damage to reputation.
	Financial	Loss of up to 5 % of revenues.
	Business	Minimum or negligible effect on achieving organisations objectives.
	People	Non-reportable minor injuries, simple first-aid
2 (Moderate)	Operation	Slight disruption to service.
	Reputation	Coverage in local media and/or some damage to reputation.
	Financial	Loss of 5 % to 30 % of revenues.
	Business	Partial failure to achieve organisations objectives.
	People	Reportable injury requiring medical treatment.
3 (Major)	Operation	Loss of service for more than 48 h.
	Reputation	Extensive media coverage and/or damage to reputation.
	Financial	Loss of over 30 % of revenues.
	Business	Non-delivery of organisations objectives.
	People	Temporary disability, hospitalisation, fatality.

Sample of qualitative measurement in the likelihood of the impacts to be materialised to the organisation.

Table A.2. Likelihood of the impact being materialised

Likelihood ratings	Likelihood of events	Description
1 (Low)	Rale/Unlikely	May likely to occur once in 10 to 50 years.
2 (Medium)	Moderate	Will occur once in 1 to 10 years.
3 (High)	Likely/Certain	Will occur at least once per year.

Annex B
(informative)

Guidelines on Business Impact Analysis (BIA) and Risk Assessment (RA)

B.1 Business Impact Analysis (BIA)

The organisation should complete a cycle of the BIA process before business continuity strategies and solutions are selected.

The BIA process analyses the effects of a disruption on the organisation. The outcome is a statement and justification of business continuity priorities and requirements.

The organisation should establish a Business Impact Assessment Procedure to provide step by step of the BIA process. The procedure should cover the following:

a) Planning for BIA.

b) Agree approach for undertaking BIA process.

c) Determine products and services' priorities with top management.

d) Determine the prioritised activities.

e) Identify resources and other dependencies.

f) Analyse and consolidate BIA results.

g) Obtain top management or the relevant committee approval for BIA results.

h) Review BIA.

Context of the organisation, roles and responsibilities and the business continuity policy should be taken as the input to the planning of BIA. The outcome of the BIA should be used to select the business strategies and solutions for the organisation's business continuity. Figure B.1 shows the guidelines of the BIA process, it's prerequisites to conduct the BIA, and the expected outcomes.

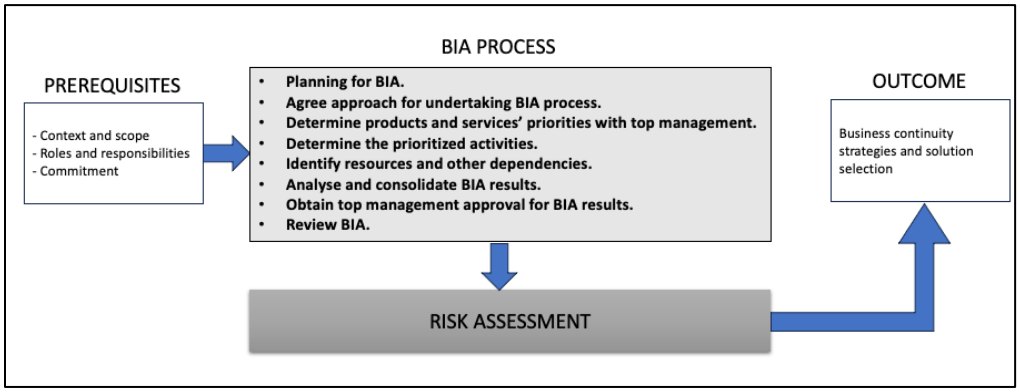

Figure B.1. Prerequisites, BIA process, RA and the outcome

B.2 Prerequisites

Before commencing the BIA process, the organisation should perform the following:

a) Define the context of the BIA process.

   i) The outcomes of the BIA process are dependent on the organisation's understanding of the internal and external context so that it can achieve its purpose by delivering its products and services to the customers.

   ii) The internal context may include of the business processes, activities and resources, as well as the potential impact caused by disruption to the delivery of products and services.

   iii) The external context may include the suppliers, and statutory and regulatory bodies in which it operates.

b) Define the scope of the BIA process.

   i) The BIA process should cover the whole of the BCM scope.

   ii) The organisation should document the defined scope of the BCM in term of its products and services. The products and services within the scope should be prioritise, those with higher priorities can be addressed first.

   iii) The outcomes of the BIA process can require the organisation to reconsider the scope of the BCM by adding of removing products and services.

c) Define and communicate roles and responsibilities.

   i) Top management should ensure the relevant roles and responsibilities are assigned, authorities are given to go certain roles who are required to make decisions on BCM.

   ii) The roles and responsibilities should be communicated within the organisation.

   iii) A BIA leader with competent should be assigned to lead the BIA process. The BIA leader is responsible to do the following.

      1) Ensure people with the required competencies are available to enable the BIA process.

      2) Prepare and deliver the BIA methodology.

      3) Plan and manage the BIA process.

      4) Ensure that the information provided by the activities owners is consistent throughout the organisation.

      5) Consolidate and analyse the information provided by the activity's owners.

      6) Present and communicate the outcomes to the top management for approval.

   iv) BIA activity owners shall be assigned to conduct the BIA. The BIA activity owners are responsible to do the following.

      1) Provide a detailed understanding of the activity for which they are responsible, including all of the resources that enable the activity to operate.

      2) Provide information regarding existing workarounds, business processes and resources

that influence the business continuity priorities and requirements.

3) Apply BIA methodology and provide the relevant information to the BIA leader.

d) Obtain top management commitment and allocated adequate resources.

i) Top management should commit to the BIA process to ensure effective participation, they should do the following:

1) Provide ongoing support for the BIA process.

2) Provide sufficient resources for BIA process.

3) Agree on the BIA methods, priorities, and time frames.

4) Ensure an environment that enables continual improvement within the organisation.

5) Approve the outcomes of the BIA that ensure the following:

- Business continuity priorities and requirements are aligned with organisation's objectives and strategic direction.

- The organisation meets its legal, contractual and customer requirements during a disruption.

- Products and services, business processes, activities and resources are appropriately aligned.

6) Ensure that BIA outcomes are available when selecting business continuity strategies and solutions.

B.3 The BIA process

a) Planning for BIA.

   i) Allocating resources including competent person to lead and participate in BIA process.

   ii) Grouping products and services with similar characteristics (by type, geographic or line of business).

      1) Identify teams or individuals (from organisation structure) that can provide information about products and services, the activities and resources to deliver these products and services.

      2) Communicating expectations to all participants in BIA process.

      3) Establish plan.

      4) Obtaining top management's agreement on the approach for undertaking the BIA process.

      5) Determine priorities of products and services with top management.

      6) Identifying and selecting the information collection methods.

      7) Defining template or tool to collect the information collected.

      8) Gathering information from the activity owners.

      9) Analysing and consolidating the information collected.

      10) Obtaining top management approval for the outcomes.

      11) Obtain approval of the planned BIA process.

b) Develop and agree the approach for undertaking BIA process.

   i) The BIA process allows the organisation to explore the impacts resulting from the disruption to the delivery of products and services to customers and other interested parties. Disruption can come from the following.

      1) Within the organisation.

      2) From the supply chain.

      3) Other external sources.

Table B.1 shows the examples of the impacts on the organisation resulting from the reactions of interested parties.

Table B.1. Prerequisites, BIA process, RA and the outcome

Interested party	Examples of the impact to the organisation
Existing customers and clients	a) Loss of revenue and market share b) Increasing complaints c) Contract penalties or litigation
Community	a) Loss of confidence b) Loss of reputation
Potential customers and clients	Loss of potential business opportunities
Partner organisations	Reduced willingness and ability to continue to cooperate
Creditors	Negative effect on debt payments and future finance requirements
Competitors	Loss of market share as competitors take advantage of the situation
Staff	Loss of key personnel (temporary or permanent)
Regulators and government	Penalties and rule changes

ii) The organisation can experience different types of impacts such as damage to reputation or business objectives, financial losses and litigation. Impact types are not the same as consequence types or categories as used in risk management. Impact is the result of a disruption on the organisation. To compare and assess impacts that are very different in a consistent manner.

iii) The organisation should define impact types and criteria to understand the impact over time of a disruption to the delivery of products and services.

iv) Top management should approve the proposed impact types and criteria. Example of impact types are as follows:

1) Business objectives.

2) Environment.

3) Financial.

4) Health and safety.

5) Legal, regulatory, and contractual.

6) Market share.

7) Operational.

8) Reputational.

v) The organisation may consider consolidating the impact types. The choice of impact types and criteria are influenced by the organisation's sector, context and the nature of its activities, as well as organisational culture. The selection of one or more impact types and criteria, including the need for quantitative and qualitative impact information and the level of detail collected, should be suitable for the organisation to select or justify business continuity priorities and requirements.

vi) To assess different types of impacts and their effect on the business, the organisation can choose to define thresholds when the impact becomes unacceptable (see the examples in Table B.2) or to define an impact matrix with defined criteria for each impact level and type (see the examples in Table B.3). The criteria should be as objective and measurable as possible.

Table B.2. Examples of thresholds for impact type (MTPD impact table)

Impact type	Description	MTPD threshold
Business objectives	Failure to deliver on objectives or take advantage of opportunities	Negative deviation by x % on business objectives (e.g., drop greater than 15%)
Financial	Financial losses due to fines, penalties, lost profits or diminished market share	Viability threatened by loss higher than MYR x in revenue or cost (e.g., loss greater than MYR 5 million)
Legal and regulatory	Litigation liability and withdrawal of license to trade	Regulator suspends operating licence (e.g., regulator suspends operating licence)
Market share	Loss of clients moving to competitors	New orders drop x % (e.g., new order drop greater than 25%)
Reputational	Negative opinion or brand damage	Leading news story (e.g., negative attention extensive enough to engage external communications experts)

Table B.3. Examples of impact label criteria

Level of impact	Impact Types						
	Financial	**Market share**	**Customer (to product/ service specific)**	**Liability (inclusive legal costs)**	**Regulatory**	**Reputational**	**Business Objectives**
1	Loss of < MYR x in revenue or expense	Loss of < x % customers to opposition	Loss of A-Service to < x % customers	Liability < MYR x < x claims	a) Little interest from regulator b) Possible request for a summary report post disruption c) Possible warning issued to public	Some negative attention in local press or in social media not requiring a response	Negative deviation < x % on business objectives
2	Loss of ≥ MYR x and < MYR y in revenue or expense	Loss of ≥ x % and < y % customers to opposition	Loss of A-Service to ≥ x % and < y % customers	Liability ≥ MYR x and < MYR y ≥ x and < y claims Class action lawsuit	a) Regulator takes an interest requesting regular updates b) Public warning issued	a) Negative attention reported via traditional news channels not requiring a response b) Social media complaints requiring response	Negative deviation ≥ x % and < y % on Business objectives
3	Loss of ≥ MYR y and < MYR z in revenue or expense	Loss of ≥ y % and < z % customers to opposition	Loss of A-Service ≥ y % and < z % customers	Liability ≥ MYR y and < MYR z ≥ y and < z claims Multiple class action lawsuits	a) Regulator on site requesting formal report b) Fines > MYR x and ≤ MYR y	a) Temporary negative regional attention reported via news channels requiring response b) Social media complaints requiring dedicated response team	Negative deviation ≥ y % and < z % on Business objectives

Table B.3. Examples of impact label criteria *(continued)*

Level of impact	Impact Types						
	Financial	**Market share**	**Customer (to product/ service specific)**	**Liability (inclusive legal costs)**	**Regulatory**	**Reputational**	**Business Objectives**
4	Loss of ≥ MYR z and < MYR t in revenue or expense	Loss of ≥ z % and < t % customers to opposition	Loss of A-Service to ≥ z % and < t % customers	Liability ≥ MYR z and < MYR t ≥ z and < t claims Multiple class action lawsuits	a) Suspension of license Fines ≥ MYR y	a) Negative national b) Attention extensive enough to engage external communications experts for traditional and social media c) Requires top management to be included in the response Pushing response video of top management through social media channels	Negative deviation ≥ z % and < t % on Business objectives
5	Loss of ≥ MYR t in revenue or expense	Business failure due to loss of ≥ t % customers to opposition	Business failure due to loss of A-Service to x zone or ≥ t % customers	Suspension of Licence Fines ≥ MYR t	Business failure due to loss of licence	a) Consistent negative media attention from traditional and social media Business failure due to perceived incompetence or loss of faith in the organisation	Negative deviation ≥ t % on business objectives

c) Define timeframes

Impacts almost always increase over time. However, different types of impact do not always increase at the same rate. For instance, financial impacts can arise as contract penalties are incurred or as customers are lost, while reputational damage can occur suddenly at a point during the disruption.

To assess the magnitude of the impact over time, the organisation can choose a set number of timeframes at which to consider the magnitude of the impact (e.g., at 1 hour, at 6 hours, at 24 hours, at 3 days, at 1 week) or a set number of time frames within which to consider the increasing magnitude of impact (e.g., 0 to 1 hour, 1 to 6 hours, 6 to 24 hours). The chosen ranges can vary between organisations depending on their context.

Figure B.2 shows the sample of the table to document the defined timeframe of the magnitude of impact over time for a product/service in relation to the different aspects of losses.

[Product / Business Activity]							
	Magnitude of impact according to the methodology defined in 2.2.4						
Impact of disruption over time	Financial Loss	Loss of Market Share	Loss of service to Customer	Liability (inclusive legal costs)	Regulatory	Reputational	Business Objectives
1 hr							
6 hrs							
24 hrs							
3 days							
1 week							

Determine the Levels of Impact based on the criteria defined in Table B.3

Figure B.2. Sample table to document the defined timeframe

d) Define methodology

A methodology should be defined to ensure that the same principles and criteria are applied when assessing all products, services and activities, regardless of when the assessment is done or the team responsible for the assessment.

The methodology should include the following.

i) How to assess impacts over time using the agreed impact types, criteria and time frames. When assessing impacts over time, the analysis should assume that the disruption occurs at the worst possible moment, e.g., the peak operating period, the end of the financial month or the busiest time of year. The worst case should be documented.

ii) Identification of the time frame when a disruption becomes unacceptable to the organisation (e.g., when at least one of the thresholds in Table B.2, or an unacceptable level of impact in Table B.3, is reached). This can be referred to as the MTPD.

NOTE: For each product and service, top management determines the threshold for the agreed impact types and selects the lowest MTPD value across the impact types (threshold).

Refer to Table B.4 for the example of identifying the MTPD for a product/service from the BIA.

iii) A set timeframe for recovery of disrupted activities with a specified minimum acceptable capacity.

This time frame can be referred to as the RTO and cannot be longer than the MTPD.

The outcomes described in this methodology are the minimum required to be consistent with ISO 22301. The organisation can add additional tasks to the BIA process, such as collecting additional information or identifying single points of failure, as part of the information-gathering sessions.

Table B.4. MTPD for product and service determined from BIA

Product or service	Impact type	MTPD threshold	Product or service MTPD
Customer service	Business objectives	48 hours	24 hours
	Financial	5 days	
	Legal and regulatory	N/A	
	Market share	N/A	
	Reputational	24 hours	
Insurance policy booklet	Business objectives	N/A	48 hours
	Financial	5 days	
	Legal and regulatory	48 hours	
	Market share	1 month	
	Reputational	1 week	

e) Determine products and services' priorities with top management.

i) Overview

Top management should determine the priorities of products and services that the organisation provides to its customers. This prioritisation can be done by discussion, although other sources of input can be available. For example, it is possible that product and service prioritisation have been previously performed as part of enterprise risk management. In these situations, the BIA process can consider those conclusions.

It is top management's responsibility to prioritise products and services because they perform the following.

1) Set the objectives of the organisation.

2) Have the ultimate responsibility for ensuring the continuity of the organisation and the fulfilment of its objectives.

3) Have the widest view of the entire organisation from which to assess priorities.

4) Can choose to override contractual and other obligations in setting priorities in exceptional circumstances.

5) Are aware of planned future changes and other factors which can affect the business continuity priorities and requirements.

ii) Inputs

To make decisions, top management should consider the following information.

1) Mission, objectives and strategic direction of the organisation.

2) BCMS scope.

3) Assessment of product and service priorities from a previous top management review.

4) Legal and regulatory requirements to which the organisation, or specific products and services, are subject (as well as an assessment of the impact of breaching each requirement).

5) Contractual requirements, including penalties for failure to deliver products and services.

6) Expectations of customers and other interested parties.

7) Assessment of impacts for failure to deliver (see impact types in B.3(b)(ii)).

8) Lessons learned from past disruptions and exercises.

iii) Determine the priority of product and service

Based on the impact types and criteria (see B.3(b)(ii)), the defined time frames (see B.3(b)(iii)) and the agreed methodology (see B.3(b)(iv)), top management should decide, for each group of products and services, the time after which continued failure to deliver them becomes unacceptable to the organisation. This determines the minimum acceptable capacity for initial recovery and how quickly it will need to return to full capacity.

When necessary, top management should also agree on the priority of internal services, such as payroll and other employee-facing services. Some organisations can choose to treat internal services similarly to externally facing products and services.

The organisation should retain documented information describing the reasons why decisions have been made.

iv) Outcomes

The outcomes should be a list of prioritised products and services and their continuity requirements which will be used in activity prioritisation (to be used as one of the inputs to determine the prioritised activities).

The outcome of the product and service prioritisation can result in the modification of the organisation's BCM scope.

f) Determine the prioritised activities.

i) Overview

It is important to understand the relationship between products and services, business processes and activities before setting the RTOs of the activities.

The priority of products and services influences the priority of their related activities. In cases where an activity is part of a business process, it is possible that the activity needs to be analysed together with the remaining activities in the business process. This can result in changes to the RTOs of activities.

ii) Inputs

The inputs required to undertake activity prioritisation include the following.

1) Scope of the BIA process.

2) Impact types and criteria (see B.3(b)(ii)).

3) Priorities for the products and services defined by top management (see B.3(e)).

4) Known dependencies.

5) Legal, regulatory, and contractual requirements (obligations).

iii) Identify activities and their owners

For each product and service within the scope of the BIA process, the related activities should be identified by their activity owners.

iv) Set RTO for the activities

Based on the impact types and criteria (see 2.2.2), the defined time frames (see 2.2.3) and the agreed methodology (see 2.2.4), activity owners should assess the impacts over time resulting from a disruption, identify the MTPD and set the RTO in combination with the minimum acceptable capacity for each activity. This capacity can be represented as a metric such as a percentage or ratio of a level of service, or quantity of product.

The information collection methods that have been identified during planning (see 2.1) and the selected template or tool should be used to document the analysis.

Each activity should be analysed, taking into consideration the following.

1) Fluctuations in demand or peak operating periods.

2) Additional factors that can affect the determination of business continuity priorities and requirements (e.g., backlogs or legal and regulatory requirements).

3) The interdependencies on other activities (internal or external).

A list of activities sorted in ascending RTO order should be created.

Table B.5 shows the example of the RTOs defined for the activities that are being identified from the Customer service against the MTPD.

Table B.5. MTPD and RTO for each activity related to customer service

Product or service	Product or service MTPD	Activity	Activity MTPD	Activity RTO
Customer service	24 hours (from Table B.5)	Front-line call handling	4 hours	1 hour
		Second line problem solving	8 hours	2 hours
		Document dispatching	24 hours	8 hours

v) Define the prioritised activities

Based on the activities' RTO, an organisation should create a list of prioritised activities.

Prioritised activities will require strategies and solutions. This requires information about resources and dependencies to be collected.

Making this selection will reduce the information to be collected but can result in no recovery solutions being defined for non-prioritised activities. In subsequent iterations of the BIA, the list of prioritised activities can be expanded.

Top management should sign off on the selection of prioritised activities.

vi) Results

The results should be as the following.

- The approved list of prioritised activities.
- For each activity:

    1) Identification of interdependencies and relationships between products and services, and activities.

    2) Impacts over time.

    3) Corresponding MTPD.

    4) Corresponding RTO.

    5) Minimum acceptable capacity.

g) Identify resources and other dependencies.

i) Identify the requirements for resource and other dependency.

After determining the prioritised activities, the organisation should obtain a detailed understanding of day-to-day resource requirements, to identify the resources necessary to recover or maintain prioritised activities. These include but are not limited to the following.

1) People.

2) Information and data (including vital records).

3) Physical infrastructure such as buildings, workplaces or other facilities and associated utilities.

4) Equipment (e.g., office equipment, manufacturing equipment, special tools, spare parts and components) and consumables (e.g., raw materials).

5) Information and communication technology (ICT) systems (e.g., applications, cloud services, remote access).

6) Transportation and logistics.

7) Finance.

8) Partners and suppliers.

ii) Resource requirements.

For the resources identified, the following information should be collected.

1) Quantity, i.e. the amount or number of resources needed over time, and based on the activity RTO, the activity owner can determine to start their activity with the following.

    - A decrease in the quantity of resources, e.g., recognising that the activity can recommence with a reduced capacity; the activity owner must then increase the quantity of resources over time so that the activity eventually returns to its business as usual.

- The business-as-usual quantity.

- An increase in the quantity of resources, e.g., to resolve the backlog accumulated over the period that the business activity was disrupted or to respond to an anticipated spike in demand. Consideration should be given to estimate the period of time the supplemental quantity of resources are to be released to return the activity to its business-as-usual level.

2) Time frame(s) in which the resources need to be available.

3) Characteristics of the resource: the information to be gathered in this case depends on the type of resources.

   - For staff and contractors, the minimum acceptable level for required service, knowledge, skills, authority, or qualifications required should be defined.

   - Specification of IT equipment.

   - Current location.

4) Maximum tolerable data loss for information resources (the RPOs should not be greater than the maximum tolerable data loss).

5) Dependencies on other resources.

6) Applicable legal or regulatory requirements.

NOTE: This information gathering can be carried out when setting the RTO for the activities.

Limitations imposed on resources, e.g., by logistics, should be taken into account when defining requirements.

During the resources requirements analysis, single points of failure can be discovered and should be documented and reported appropriately.

Table B.6 shows the example of resources required for the front-line call handling of customer service.

Table B.6. Resources required for front line call handling activity

Activity	Front line call handling
Activity RTO	1 hour
Product(s) and service(s) delivered	Customer service
Interdependencies	New pricing from consumer products department
Resources	a) Staff b) Equipment c) Applications d) Suppliers

Resources required for each activity may not be required in full during disruption while restoration of such service is in progress. Table B.7 shows the accumulative staff numbers required over time.

Table B.7. Cumulative staff numbers required over time

Activity	Resource	BAU*	1 hour	<2 hours	<8 hours	<1 week	<1 month	>1 month
Front-line call handling	Supervisors	6	1	1	2	4	4	6
	Operators	100	5	15	40	80	80	100
Second line problem solving	Supervisors	4	0	1	1	2	2	4
	Software engineers	30	0	5	12	20	20	30
Document dispatching	Operators	5	0	1	1	1	3	5
Total		145	6	22	56	107	109	145
* BAU is business as usual.								

For system dependency, the RTO and RPO requirements shall be defined, Table B.8 shows the example of the list of applications required with their RTO and RPOs to support the activities. For more comprehensive guidelines for business continuity in information and communication technology, please refer to ISO/IEC 27031, *Information Technology - Security Techniques - Guidelines for information and communication technology readiness for business continuity*.

Table B.8. Example for the list of applications required within their RTO and RPOs

Application	Used by activity	RTO from activity	Application RTO	RPO from activity	Application RPO
Call register system	Front-line call handling	1 hour	1 hour	2 hours	2 hours
	Second line problem solving	2 hours		12 hours	
Call handler system	Front-line call handling	1 hour	1 hour	24 hours	24 hours
Document management repository	Document dispatching	24 hours	24 hours	24 hours	24 hours

Table B.9 shows the list of suppliers that are required to support the activities and the resource RTO required from the suppliers.

Table B.9. List of suppliers and their resource RTO

Supplier	Resource	Used by activity	Activity RTO	Resource RTO
Supplier A	External call operators	Front-line call handling	1 hour	24 hours
	Software engineer	Second line problem solving	2 hours	5 days
Supplier B	Courier	Document patching	24 hours	48 hours

h) Analyse and consolidate BIA results

While analysis occurs throughout the BIA process, the organisation should perform a final analysis (or consolidation of analyses). This involves reviewing validated and approved information gathered from all levels of the BIA process and drawing conclusions that lead to business continuity priorities and requirements.

The organisation should choose the appropriate quantitative and qualitative analytical approach(es), which can be influenced by the type, size or nature of the organisation, as well as resource and skill constraints. The approach(es) selected will also depend on the type of information gathered.

Regardless of approach, the organisation should challenge and check the information to ensure that it is as the following.

i) Correct: sufficiently accurate and reliable.

ii) Credible: reasonable and justifiable.

iii) Consistent: comparable, clear and repeatable.

iv) Current: up to date and available in a timely manner.

v) Complete: comprehensive.

The consolidation can reveal incompatible or inappropriate recovery objectives that need to be reviewed with the activity owner and resolved. Furthermore, it can be necessary to adjust the RTO of predecessor activities to ensure successor activities can meet their set RTOs.

The results of analysing and consolidating information are the business continuity priorities and requirements.

i) Obtain top management approval for the BIA results

The BIA leader should seek management approval of BIA results, including the prioritisation of products and services, business processes (if applicable), activities and resources.

The organisation should provide the following key BIA results to top management for their review, amendment (if necessary) and approval before moving on to next steps.

i) Product and service prioritisation.

ii) Business process prioritisation (if undertaken).

iii) Activity prioritisation.

iv) Confirmation of the original, or endorsement of the modified, BIA scope.

The approval of the BIA results by top management should be documented. Some organisations can choose to seek approval via a report or presentation to top management. A presentation should be chosen if the organisation would benefit from debating the BIA results before approving or proposing an alternate conclusion. A report can be appropriate as a pre-read to a presentation or as the primary method of seeking approval, if recommended business continuity priorities and requirements and their justification are straightforward and likely not to require discussion.

The BIA results are used to identify and select business continuity strategies and solutions.

B.4 Review BIA results

a) Review BIA process and methodology

The BIA process and methodology should be reviewed to continually improve its quality. Different approaches over time can be considered, changing, for example, impact types, time frames, information collection methods or participants to improve the quality of the results.

b) Review BIA results

BIA results should be reviewed on a periodic basis (typically annually) and whenever there are significant changes within the organisation or the context in which it operates that can affect the business continuity priorities and requirements, such as the following.

i) Mergers and acquisitions.

ii) Strategic directional changes.

iii) Product or service changes.

iv) Regulatory changes.

v) Customer and/or contractual changes.

vi) Operational changes, including new or change application or ICT, supply chain (insourcing or outsourcing) and site or facility resources.

vii) Changes to the organisation's structure.

viii) lessons arising from business continuity exercises and disruptions.

The activity owners should monitor their activities, and top management should consider strategic changes to identify these triggers.

In areas of the organisation which have changed little since the last BIA, it can be sufficient to validate the previous BIA results rather than conduct a full BIA.

B.5 Risk Assessment (RA) for business continuity

Although business continuity risk assessment and BIA are different processes, it is common to identify business continuity risks while conducting the BIA, especially when carried out through interviews. In addition, the identification of resources necessary to perform the prioritised activities also provides the organisation with an important input for risk assessment, e.g., the risk of unavailability of any of those resources. Also, during a BIA interview or during the resource requirements analysis, the impact of single points of failure or unacceptable levels of risk can be revealed.

The identified risks should be analysed outside the BIA process and within the scope of the business continuity risk assessment.

The goal of conducting a risk assessment is to empower the organisation to evaluate the potential disruptions to its prioritised activities and subsequently take suitable measures to mitigate these risks.

The organisation is expected to establish and uphold a formal risk assessment procedure. This procedure should systematically identify, analyse, and assess the risks associated with the interruption of the organisation's prioritised activities, along with the associated processes, systems, information, personnel, assets, suppliers, and other supporting resources.

A risk assessment involves a methodical approach to evaluating risks, considering both their likelihood and potential consequences, before making decisions regarding any necessary additional risk management actions.

The complete risk assessment guidelines should be referred to the ISO/IEC 31000. This document will provide examples of threats.

The scale of likelihood and the scale of impacts for the BCM can be referred to Annex A.

B.6 List of threats

Natural and man-made threats can cause disruption to an organisation's operations or services.

This is a list of possible threats to an organisation. From this list, the Organisation BCM Coordinator and the BC Team are required to identify and extract the likely and high-impact threats that will affect your organisation. Sometimes, this list of threats may be reorganised into three primary categories of internal and external threats: malicious activities, natural disasters and technical disasters.

Denial of Access can be man-made or natural and includes all threats that will result in the denial of access/availability to people, processes, infrastructure, and partners/suppliers. This could range from a flood keeping you from entering the office premises to a power outage disrupting work.

Table B.10 provides the list of possible threats.

B.10. List of threats

Threats	Natural / man-made	Examples of threats		
Denial of access	Both	a) Blizzard b) Clouds c) Cyclone d) Drought e) Dust storm f) Flood g) Flash flood h) Fog/haze i) Heat wave j) Hurricane	k) Lightning l) Rain m) Snow n) Thunder o) Tornado p) Tropical storm q) Typhoon r) Weather front s) Waterspout t) Wind	u) Windstorm v) Fire storm w) Fire - wild, rural or urban x) Terrorism y) Bomb threat or explosion z) Power outage aa) Earthquake tremors
Unavailability of people	Both	a) Labour dispute/strike b) Infectious disease/ pandemic c) Workplace safety d) Workplace violence	e) Loss of key appointment holders f) Mishandling of hazardous materials g) Haze	
Disruption of supply chain	Both	a) Loss of specialised vendor/ partner/ supplier (i.e. aviation, rail, maritime, vehicular)	b) Regulatory or legal violation c) Default of key debtors d) Accidents	
Equipment and IT-related disruption	Both	a) IT failure (i.e. hardware, software) b) Network failure (i.e. local and wide network) c) Telecommunications failure (phone line)	d) IT sabotage e) Facilities and equipment failure (i.e. air-con, lift, transformer, HVAC, UPS, backup generator)	
Meteorological	Natural	a) Blizzard b) Clouds c) Cyclone d) Drought e) Dust storm f) Flood g) Flash flood h) Fog/haze	i) Heat wave j) Hurricane k) Lightning l) Rain m) Snow n) Thunder o) Tornado p) Tropical storm	q) Typhoon r) Weather front s) Waterspout t) Wind u) Windstorm v) Fire storm w) Fire - wild, rural or urban

B.10. List of threats *(continued)*

Threats	Natural / man-made	Examples of threats		
Social	Man-made	a) Individual behaviour b) Mass behaviour c) Terrorism d) Hijacking in individual, VIP or group e) Assassination	f) Torture g) Poisoning h) Wounding i) Bomb j) Bomb threat k) Car bomb l) Suicide bomb	m) Improvised Explosive Device (IED) n) Biological o) Nuclear p) Chemical q) Cyber
Technological	Man-made	a) Transportation related events b) Aviation accident on air and ground c) Rail accidents occurring above or below ground d) Maritime accidents on port, near cost and off the coast e) Vehicle accidents f) Car accident g) Multiple car accident h) Bus accident	i) Information technology related events j) Hardware malfunction k) Software malfunction l) Hazardous materials related events m) During production n) During transportation by road, air, rail, pipeline and sea o) During storage p) Supply related events	q) Utilities r) Power energy s) Communications t) Water u) Gas v) Oil w) Gasoline x) Food y) Basic services z) Security services aa) Safety services bb) Health services cc) Transportation services
Medical	Man-made	a) Epidemiology b) Pandemic flu c) Dengue fever		
Geological	Natural	a) Endogenic b) Plate Tectonics c) Earthquake d) Igneous Activity e) Volcanic Eruption	f) Exogenic g) Slope h) Mass Wasting i) Landslide j) Flow	k) Avalanche l) Mudslide m) Weathering n) Erosion

Bibliography

[1] *MS 1970, Malaysia Business Continuity Management Framework*

[2] *ISO/IEC 22301, Societal security - Business continuity management systems - Requirements*

[3] *ISO/IEC 22313, Business continuity management systems - Guidance*

[4] *ISO/IEC 27031, Information technology - Security techniques - Guidelines for information*

[5] *Business Continuity Management for Singapore's Logistics Sector*

[6] *Disaster Recovery Institute International (DRII) Professional Practices for Business Continuity Practitioners*

[7] *Good Practice Guidelines 2018, Edition by Business Continuity Institute (BCI)*

[8] *Guidelines on Business Continuity Management (BCM), Bank Negara Malaysia*

[9] *Swiss Banking, Recommendations for Business Continuity Management (BCM)*

Acknowledgements

Members of the Fundamentals Security Technologies Sub Working Group

Mr Ong Yew Seng (Chair/Draft Lead)	Digiforen (M) Sdn Bhd
Mr Robin Yong Hong Cheng (Vice Chair)	U Mobile Sdn Bhd
Ms Norkhadhra Nawawi (Secretary)	FNS (M) Sdn Bhd
Mr Khairul Ekhwan Kamarudin (Secretariat)/ Ms Alisa Rafiqah Adenan (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Ahmad Akmal Syahmi/ Mr Azlan Mohamed Ghazali	Deloitte Business Advisory Sdn Bhd
Mr Jerry Yap Tsok Shen	Digital Nasional Berhad
Mr Wan Ameer Ruzman	FNS (M) Sdn Bhd
Ms Caroline Pitchaymuthu/ Mr Zulkifli Mohd Aini	Maxis Broadband Sdn Bhd
Ms Jamalina Othman/ Mr Victor Low Choon Hee	TM Technologies Services Sdn Bhd
Ms Nur Liyana Abdul Razak	U Mobile Sdn Bhd
Professor Dr Shahrulniza Musa/ Dr Ahmad Shahrafidz Khalid/ Dr Amna Saad	Universiti Kuala Lumpur

By invitation:

Ms Magdalena Ognenoska	Axiata Group Berhad
Mr Mahadevan @ Kannan AL Sivaswamy	CIMB Group Holdings Berhad
Ms Khaw Peg Gie	KPMG Malaysia
Ms Azreena Mohd Norawi Mr Syarifuddin Palawa	Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia
Ms Nisha Hanina Abd Rahim/ Ms Norsyila Awang Bakar	UMW Holdings Berhad
Ts Woo Yuen Seng	Yswoo BCP & IT Consultancy