MCMC MTSFB TC G014:2018

TECHNICAL CODE

BUSINESS CONTINUITY MANAGEMENT (BCM) - REQUIREMENTS

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date:

15 October 2018

MCMC MTSFB TC G014:2018

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
http://www.skmm.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Malaysian Communications & Multimedia Commission (MCMC)
Off Persiaran Multimedia
Jalan Impact
Cyber 6
Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8320 0300
Fax: +60 3 8322 0115
http://www.mtsfb.org.my

Contents

Page

Committee representation iii
Foreword iv

0. Introduction 1
1. Scope 2
2. Normative references 2
3. Terms and definitions 2
   3.1 Business continuity management 2
   3.2 Business Continuity Plan (BCP) 2
   3.3 Business Impact Analysis (BIA) 2
   3.4 Business recovery 2
   3.5 Critical business functions 2
   3.6 Interested party 2
   3.7 Maximum Tolerable Period of Disruption (MTPD) 3
   3.8 Minimum Business Continuity Objective (MBCO) 3
   3.9 Recovery Point Objective (RPO) 3
   3.10 Recovery strategies 3
   3.11 Recovery Time Objective (RTO) 3
   3.12 Risk appetite 3
   3.13 Risk assessment 3
   3.14 Top management 3
4. Abbreviations 4
5. Context of organisation 4
   5.1 Purpose of Business Continuity Management System (BCMS) 4
   5.2 Scope of Business Continuity Management System (BCMS) 5
6. Leadership 5
   6.1 Management commitment 6
   6.2 Policy 6
   6.3 Responsibilities 7
7. Planning 7
   7.1 Addressing risks 7
   7.2 Business continuity objectives 8
8. Support 8
   8.1 Business Continuity Management System (BCMS) resources 9
   8.2 Incident response personnel 9

8.3 Competence 9
8.4 Awareness 10
8.5 Communication 10
8.6 Document control and change management 10
9. Operations 11
9.1 Operational planning and control 11
9.2 Risk assessment (RA) and Business Impact Analysis (BIA) 12
9.3 Business continuity strategies 13
9.4 Establish and implement business continuity procedures 14
9.5 Exercising and testing 17
10. Performance evaluation 18
10.1 Monitoring, measurement, analysis and evaluation 18
10.3 Internal audit 19
10.4 Management review 19
11. Improvement 20
11.1 Non-conformity and corrective action 20
11.2 Continual improvement 21

Annex A Sample of qualitative measurement 22
Bibliography 23

Committee representation

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

Celcom Axiata Berhad

Kementerian Sains, Teknologi dan Inovasi

Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia

Provintell Technologies Sdn Bhd

Telekom Applied Business Sdn Bhd

Telekom Malaysia Berhad

TIME dotCom Berhad

Universiti Kuala Lumpur

webe digital sdn bhd

Foreword

This technical code for Business Continuity Management (BCM) - Requirements ('this Technical Code') was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd (MTSFB) via its Trust and Privacy Sub Working Group. It defines the general requirements to establish, maintain and implement effective business continuity plan as an extension to the document 'MCMC MTSFB TC G009:2016'.

Many BCM documents related to the requirements and guidelines available for reference. These documents are international standards, professional best practice, federal guidelines and federal regulations or directive. This technical code standardises the terms used in other organisations in order to achieve the common understanding while implementing the Business Continuity Management System.

This Technical Code shall continue to be valid and effective until reviewed or cancelled.

BUSINESS CONTINUITY MANAGEMENT (BCM) - REQUIREMENTS

0. Introduction

Any major incident that escalates to disaster could have a significant business impact over time on the organisation.

The Business Continuity Management (BCM) implementation (see Figure 1) is expected to provide the following benefits:

a) provide a structured approach of managing risk within the organisation's environment;

b) provide strategic plan to respond and recover from risks that cannot be controlled or mitigated;

c) provide business continuity and minimise damages and losses under adverse or abnormal conditions;

d) reduce negative impact to business objectives;

e) encourage improved collaboration between its interested parties;

f) provides assurance to top management and interested parties that it can depend upon predetermined levels of services in the event of a disruption;

g) enhance the organisation's reputation for prudence and efficiency; and

h) potentially gains competitive advantage through the demonstrated ability to deliver business continuity and maintain product and service delivery in the event of disruption.

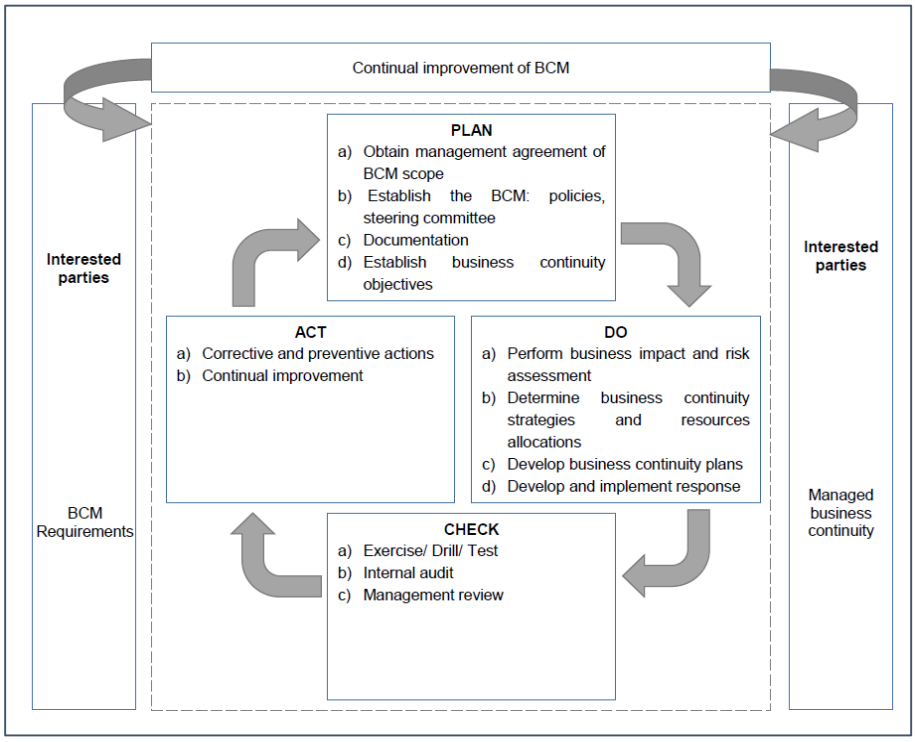

Figure 1. BCM implementation cycle

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 31000, *Risk management - Principles and guidelines*

3. Terms and definitions

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

3.1 Business continuity management

Holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key interested party, reputation, brand and value creating activities.

3.2 Business Continuity Plan (BCP)

Documented procedures that guide organisations to respond, recover, resume and restore to pre-defined level of operation following a disruption.

This covers resources, services and activities required to ensure the continuity of critical business functions.

3.3 Business Impact Analysis (BIA)

Process of analysing activities and the effect that a business disruption might have upon them.

3.4 Business recovery

The courses of action for rebuilding functions to the condition where they are ready to maintain product and service delivery. This condition should be at a level sufficient to meet minimum business continuity objective.

3.5 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.

3.6 Interested party

Person or organisation that can affect, be affected by or perceive themselves to be affected by a decision or activity.

NOTE. This can be an individual or group that has an interest in any decision or activity of an organisation.

3.7 Maximum Tolerable Period of Disruption (MTPD)

Time it would take for adverse impacts, which might arise as a result of not providing critical business functions or performing an activity, to become unacceptable.

NOTE. Some standards or best practice documents use Maximum Tolerable Downtime (MTD).

3.8 Minimum Business Continuity Objective (MBCO)

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

3.9 Recovery Point Objective (RPO)

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

3.10 Recovery strategies

An approach by an organisation that will ensure its recovery and continuity in the face of a disaster or other major outage. 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 etc.)

3.11 Recovery Time Objective (RTO)

The duration of time from the activation of the Business Continuity Plan (BCP) to the point when the specific business function is recovered. It is the acceptable duration of time that can elapse before the non-continuation of the specific business function would result in severe business impact and losses to the organisation.

3.12 Risk appetite

Amount and type of risk in an organisation are willing to pursue or retain.

3.13 Risk assessment

Process of identifying the risks to an organisation, assessing the critical functions necessary for an organisation to continue its business operations. Risk analysis often involves an evaluation of the probabilities and severities of a particular event.

3.14 Top management

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

Top management has the power to delegate authority and provide resources within the organisation. If the scope of the BCMS covers only part of an organisation then top management refers to those who direct and control that part of the organisation.

4. Abbreviations

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

BCMS	Business Continuity Management System
BCP	Business Continuity Plan
BIA	Business Impact Analysis
ICT	Information and Communications Technology
IT	Information Technology
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

5. Context of organisation

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 BCMS. These issues refer to establishing the external and internal context of the organisation considered in ISO 31000.

5.1 Purpose of Business Continuity Management System (BCMS)

The key purpose of implementing BCMS is to protect the following against disasters and major disruptive events:

a) people:

   i) ensure the safety of employees and interested parties; and

   ii) provide humanitarian relief of employees and interested parties.

b) key interested parties:

   i) shareholders;

   ii) investors;

   iii) customers;

   iv) business partners;

   v) contractors;

   vi) suppliers; and

   vii) visitors.

c) key information and physical assets; and

d) critical business functions and supply chain.

The corporate level Minimum Business Continuity Objectives (MBCO) shall be established based on the key purpose. The key purpose of BCMS and the corporate MBCOs provides the key criteria with which the BCP will be implemented. Therefore, these shall be clearly communicated to and understood by an interested party.

5.2 Scope of Business Continuity Management System (BCMS)

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

When determining the BCMS scope the organisation shall:

a) identify the functional parts to be included in the BCMS;

b) establish the BCMS requirements taking into consideration its mission, goals, legal responsibilities and internal and external obligations;

c) identify the products and services in a manner that enables all related activities, resources and supply chains to be identified;

d) take into account the needs and interests of the interested party; and

e) identify the applicable legal and regulatory requirement related to the continuity of its operation, product and services.

The BCMS scope shall be established for a limited scope covering important business and support operations at specific sites. The business continuity should be flexible, adaptable and scalable to increase the BCMS capabilities and competency over time.

BCMS scope shall also:

a) include an indication of the incident scale that the BCMS will address and the organisation's risk appetite; and

b) identify how the BCMS fits into the organisation's overall risk management strategy.

Where part of an organisation is excluded from the scope of its BCMS, the organisation shall document the exclusion as determined by Business Impact Analysis (BIA) and applicable legal or regulatory requirements.

6. Leadership

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

Top management is responsible to ensure the development, implementation, maintenance and effectiveness of the BCMS in the organisation.

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

6.1 Management commitment

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

a) complying with applicable legal, regulatory and other requirements to which the organisation subscribes;

b) integrating BCMS 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 BCMS and accountable for its effective operation;

e) ensuring that BCMS 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 BCMS audits are conducted;

i) ensuring regular management reviews of the BCMS;

j) directing and supporting the improvement of the BCMS;

k) operational involvement through steering groups; and

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

6.2 Policy

Top management is responsible for steering BCMS 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:

a) is appropriate to the purpose of the organisation;

b) provides a framework for setting business continuity objectives;

c) includes a commitment to satisfy applicable requirements; and

d) includes a commitment to continual improvement of BCMS.

The BCMS 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 Responsibilities

The organisation shall also establish a dedicated BCMS steering committee which consists of relevant top management. The BCMS working committee that is led by business continuity manager, who is responsible to support and provide feedback to BCMS steering committee.

The working committee shall comprise a BCMS coordinator who is assigned to monitor the business continuity and representatives which include, but not limited to:

a) critical business units;

b) Information Technology (IT);

c) internal audit;

d) legal and regulatory;

e) human resource;

f) security;

g) property management and services;

h) corporate and services/communication; and

i) customer service.

The organisation shall retain a documented information that defines the roles and responsibilities of individuals and/or committee responsible for BCMS.

7. Planning

7.1 Addressing risks

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

a) ensure the management system can achieve its intended outcome(s);

b) prevent, or reduce, undesired effects; and

c) achieve continual improvement.

The organisation shall plan:

a) action to address these risks; and

b) how to:

   i) integrate and implement the actions into its BCMS processes; and

   ii) evaluate the effectiveness of these actions.

7.2 Business continuity objectives

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

The business continuity objectives shall:

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; and

f) be monitored and updated as appropriate.

To achieve its business continuity objectives, the organisation shall determine:

a) roles and responsiblities;

b) what will be done;

c) resources required;

d) when it will be completed; and

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 BCMS that will:

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; and

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 System (BCMS) resources

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

a) people and people related resources, including:

   i) the time necessary to fulfil BCMS roles and responsibilities;

   ii) training, education, awareness and exercising; and

   iii) management of BCMS 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; and

f) finance and funding.

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

8.2 Incident response personnel

The organisation shall nominate incident response personnel with the necessary responsibility, authority and competence to manage an incident.

The incident response personnel shall form a team that is responsible for managing any disruptive incident that significantly impacts or has the potential to significantly impact the organisation.

Team members shall be assigned accordingly to their demonstrated competence of dealing with different aspects of incident response, for example:

a) incident management/strategic management;

b) communications;

c) safety and humanitarian relief;

d) salvage and security;

e) resuming activities; and

f) recovery of services.

All members who are on these teams shall have clearly defined responsibilities and authorities that apply before, during and after an incident.

8.3 Competence

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

Management shall determine the competencies required for all BCMS roles and responsibilities and the awareness, knowledge, understanding, skills and experience needed to fulfil them. All assigned personnel with BCMS 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.

8.4 Awareness

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

a) the business continuity policy;

b) their contribution to the effectiveness of the BCMS, including the benefits of improved business continuity management performance;

c) the implications of not conforming to the BCMS requirements; and

d) their own role and responsibility during disruptive incidents.

Management shall progressively promote an organisational culture that places a high priority on enhancing business continuity capability and ensures BCMS 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 BCMS.

8.5 Communication

The organisation shall establish a communication plan that includes:

a) internal communications within employees within the organisation;

b) external communications within the interested party, partners, customers, local community as well as media;

c) ensuring the availability of the means of communication during the disruptive incident; and

d) operating and testing of communications capabilities intended for use during disruption of normal 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.

8.6 Document control and change management

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

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

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:

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 BCMS;

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; and

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 2 illustrates the elements of operational planning and control.

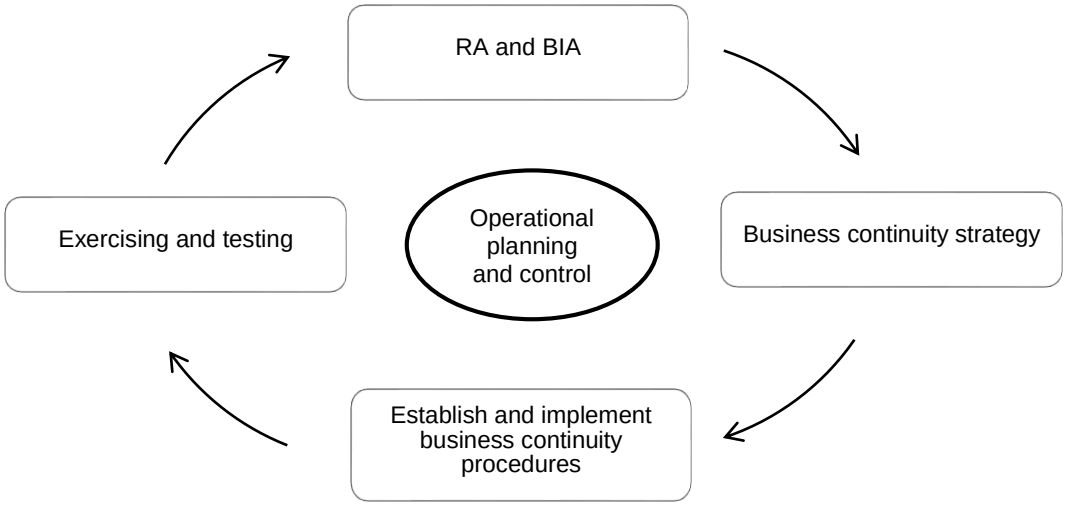

Figure 2. Elements of operational planning and control

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/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/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; and

e) interdependencies and dependencies between business areas and/or interested party.

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

Based on the BIA results, the organisation shall determine the MBCO, Maximum Tolerable Period of Disruption (MTPD) and Recovery Time Objective (RTO) for each critical business function. 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 MBCO, MTPD and RTO shall correspond with the importance and criticality of the business functions. The organisation shall establish MBCO 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.

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.

Figure 3 illustrates the relationship between RPO, RTO, MBCO and MTPD.

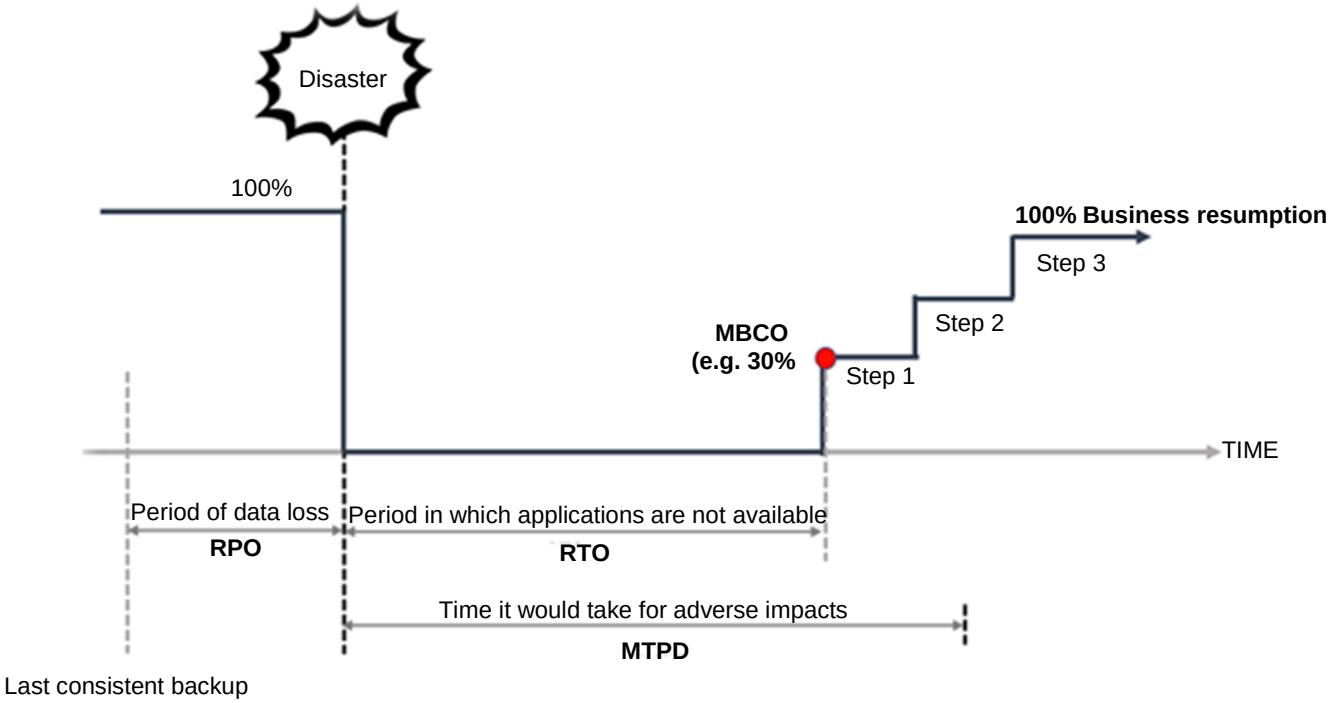

Figure 3. RPO, RTO, MBCO and MTPD concept

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

9.3 Business continuity strategies

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:

a) reduce the likelihood of disruption;

b) shorten the period of disruption; or

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; and

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; and

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

9.4 Establish and implement business continuity 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. The business continuity procedures shall establish the appropriate internal and external communications protocol and be:

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.

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 BCM certified consultant.

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; and

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 MBCO) to adequately support the critical business functions; and

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/MBCO and for critical business functions.

For the use of an interested party alternate site or recovery facility, the organisation shall:

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; and

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.

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; and

g) disposed of using established procedures.

9.5 Exercising 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 any of the following:

a) desktop walk through exercise to full system test;

b) staff call-tree activation (with and without mobilisation);

c) backup site to backup site exercise (including with it or disaster recovery service providers);

d) alternative arrangements of shared services;

e) backup disk restoration; or

f) retrieval of vital records.

Formal exercise documentation and debrief, post mortem 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:

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; and

g) recommending remedial actions for future tests.

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

10. Performance evaluation

10.1 Monitoring, measurement, analysis and evaluation

The procedures for the performance and the effectiveness of the BCMS 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; and

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 BCMS with applicable legislation, statutory and regulatory requirements; and

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 Evaluation of business continuity procedures

The organisation shall conduct evaluations of its business continuity procedures in order to ensure their continuing suitability, adequacy and effectiveness.

The evaluations shall address the possible need for changes to policy, objectives, strategies, and other elements of the BCMS considering the exercise results, post incident reviews, changing circumstances and the commitment to continual improvement.

The evaluations shall take the form of internal or external audits. The frequency and timing of reviews shall be influenced by laws and regulations, depending on the size, nature and legal status of the organisation. They might also be influenced by the requirements of interested parties.

A clearly defined and documented maintenance programme shall be established.

The outcomes from the maintenance process shall include:

a) documented evidence of the proactive management and governance of the organisation's BCMS;

b) verification that key people that will implement the business continuity strategy and procedures are trained and competent;

c) verify the effectiveness of the operational planning and control of BCMS (refer clause 10.1);

d) evidence that the organisation has evaluated compliance with its business continuity procedures; and

e) evidence that significant changes to the organisation's structure, products and services, and activities have been reflected in the organisation's business continuity procedures in a timely manner.

10.3 Internal audit

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

Internal auditors shall review the level of commitment to BCMS and overall preparedness against the organisation's BCMS 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.

10.4 Management review

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

Management review shall include an appraisal of:

a) the status of actions from previous reviews;

b) the performance of the BCMS 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 BCMS; and

d) opportunities for continual improvement.

Personnel who are involved in implementing the BCMS 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 BCMS and shall result in the following changes:

a) variations in the scope;

b) improvements in its effectiveness;

c) updates to business continuity procedures; and

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:

a) communicate the results of management review to the relevant interested party; and

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 consequences 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; and

   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 BCMS are identified and communicated in a timely manner to prevent further occurrence of the situation;

d) identify and address root causes; and

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 BCMS to a higher level of effectiveness by monitoring and reviewing the organisation's BCMS 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	Consequences 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.

Bibliography

[1] MS 1970: 2007, *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] *Business Continuity Management for Singapore's Logistics Sector*

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

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

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

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

Acknowledgements

Members of the Trust and Privacy Sub Working Group

Mr Yew Seng Ong (Chairman)	Provintell Technologies Sdn Bhd
Mr Ahmad Taufik Nik Nor Azlan (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Azlan Mohamed Ghazali	Celcom Axiata Berhad
Ms Faridah Ibrahim	Kementerian Sains, Teknologi dan Inovasi
Mr Syarifuddin Palawa	Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia
Mr Nicholas Ng	Provintell Technologies Sdn Bhd
Mr Thaib Mustafa	Telekom Applied Business Sdn Bhd
Mr Mohd Azrin Muhamad Nor/	Telekom Malaysia Berhad
Mr Mohd Shahrul Azamer Rumli/	
Ms Rafeah Omar/	
Mr Mohamad Azhar Abdullah	
Mr Wan Ahmad Ezani Wan Mohamed	TIME dotCom Berhad
Prof Dr Shahrulniza Musa/	Universiti Kuala Lumpur
Ms Roziyani Rawi/	
Mr Shadil Akimi Zainal Abidin	
Ms Farah Nuamirha Mohamad/	webe digital sdn bhd
Mr Haizam Abu Hassan	