Business Continuity Management Standard and Guide

AE/HSC/NCEMA 7000: 2012

Version 1

His Highness Sheikh

Khalifa Bin Zayed Al Nahyan

President of the United Arab Emirates

Chairman of the Supreme Council for National Security

His Highness Sheikh

Mohammed Bin Rashid Al Maktoum

Vice President and Prime Minister of the UAE and Ruler of Dubai

Vice Chairman of the Supreme Council for National Security

His Highness Sheikh

Mohammed Bin Zayed Al Nahyan

Crown Prince of Abu Dhabi

Deputy Supreme Commander of the UAE Armed Forces

Member of the Higher National Security Council

His Highness Sheikh

Hazza Bin Zayed Al Nahyan

National Security Advisor

Chairman of NCEMA Board

United Arab Emirates
The Supreme Council for National Security
National Emergency Crisis and Disasters Management Authority (NCEMA)

Business Continuity Management

Standard and Guide

AE/HSC/NCEMA 7000: 2012

Version 1

Use Key

This book is a standard benchmark to build an entity's capability to continue functioning and delivering its core services in times when emergencies disrupt or stop its business.

Part 1 **Specifications**
Includes the specifications, and sets out all key parts and elements of the program.

Part 2 **Guide**
Interprets clearly "how" the elements mentioned in part 1 work. The sections in part 2 reflect their counterparts in part 1, bearing the same numbering system. For example, paragraph 8-2-1 in part 1 corresponds to paragraph A-8-2-1 in part 2, etc.

Part 3 **Toolkit**
Includes sample BCM templates. We have set one template for the business continuity plan as an example that can be used. When updates are made in the future, we will set other supporting templates.

This standard doesn't contradict with any other document issued by the National Emergency Crisis and Disaster Management Authority (NCEMA). In case of any contradiction, please refer to the documents concerned and follow them. This "Standard" and "Guide" are only to manage business continuity. This document is a "Standard" to manage business continuity.

Preface:

The development and issuance of this standard took roughly eighteen months. The project was initiated in early September 2009. A respectable number of bodies, companies, global experience houses together with numerous global specialists took part in producing this Standard, under the leadership and supervision of the National Emergency Crisis and Disaster Management Authority (NCEMA) that is operating under the umbrella of the Supreme Council for National Security.

Participating Bodies in Standard development:

- A team from the National Emergency Crisis and Disaster Management Authority

- Members from Abu Dhabi Executive Council
- Specialists from Abu Dhabi Accountability Authority (ADAA)
- Members from Abu Dhabi Information Center

Bodies participating in the specialized review of the Standard:
- British Standards Institute (BSI)
- Business Continuity Institute (BCI)
- Disaster Recovery International Institute (DRII)

Bodies participating in technical review:
- Office of the Supreme Deputy Commander of the UAE Armed Forced
- Office of the Chief of Staff of the Armed Forces
- Ministry of Interior
- Ministry of Foreign Affairs
- General Department of State Security
- Ministry of Health
- Ministry of Transport
- Ministry of Labor
- Ministry of Energy
- Ministry of Economy
- General Civil Aviation Authority
- Securities and Commodities Authority
- Telecommunications Regulatory Authority
- Federal Electricity & Water Authority
- Chamber of Commerce and Industry
- Federal Authority for Nuclear Regulation
- Supreme Petroleum Council
- National Media Council
- Federal Customs Authority
- Central Bank of the U.A.E
- General Information Authority

Table of Contents

Forward by

H.H. The National Security Advisor

As our wise leadership endeavors to ensure the welfare and stability of the society at all times, we spare no effort to empower all UAE entities, in all vital sectors, to perform their services and duties towards the society. This should not be restricted to normal conditions but should extend to include the capability to deal with sudden incidents by developing well-rounded and pre-coordinated plans. In doing so, such entities would be able to continue performing their role and duties towards the community, when a disaster occurs.

This document is produced to serve as a guidance standard to help all entities in the field of business continuity management. Our experts and specialists revised the global best practices in business continuity and we deemed it necessary to produce this standard to be used as a reference to help all public and private entities reach the required level of performance and achieve the flexibility and capability of addressing sudden incidents as well as continuity of business during emergencies and crises.

Today, business continuity management is being unquestionably recognized as an increasingly important element in the emergency and crisis management process. Building this capability requires support and encouragement by top management to ensure additional resources are put into use, which would help the entity continue performing its critical and essential functions during an emergency until full recovery.

In this context, we call on everyone to cooperate and comply with this standard, so as to ensure the minimum technical, training, and administrative requirements are satisfied, providing reassurance and stability for the community at all times.

May God's blessings alight upon our endeavors to protect our country and people under the umbrella of our wise leadership.

Shiekh Hazza Bin Zayed Al Nahyan

Introduction

Under the guidance and direction of the wise leadership and the UAE federal government which continuously strive to maintain and enhance the stability of the country, with the ongoing follow up of the Supreme Council for National Security, the National Emergency Crisis and Disaster Management Authority (NCEMA) has drafted the first version of the Business Continuity Management Standard.

This BCMS, BC Guide and BCM Toolkit have been developed to help entities systematically build their business continuity capability during and after an emergency, disaster or crisis. All these initiatives are aimed at ensuring ongoing performance of essential functions and services in both the public and private sectors, for the purpose of enhancing the UAE's national stability.

Government entities and its private -sector partners should effectively handle emergencies and crises in a well-coordinated manner in order to fully recover from such a situation. Service delivery shall not be disrupted when an emergency occurs until recovery is completed.

Business Continuity Management (BCM) refers to building the entity's capability to continue performing essential functions and services (at a minimum) in and after an emergency, crisis or disaster that could have resulted in a business disruption.

The first BCM standard was drafted in 2006 in the UK after having endured large-scale crises and disasters. Researchers thus found themselves compelled to find mechanisms and methods to develop BCM standards. Should the entities comply with such standards, they will continue delivering critical/ essential functions and services, recover from the disruption, and return to normal operations. United Arab Emirates is a leading nation in this field since there is no BCM standard in Arabic in any country in the region.

The business continuity management objectives of the UAE government or local governments of each emirate and the entities under their jurisdiction in both public and private sectors are as follows:

- Maintain continuity of main / essential works and services in both public and private sectors including non-profit organizations.
- Secure chain of supply required for business continuity.

- Set up effective business continuity plan for delivering main / essential services when an emergency occurs in a planned and controlled manner.
- Develop proactive business continuity and risk management plan in day-to-day activities and services at all federal and local entities in the emirate, and the entities under their jurisdiction in both public and private sectors.

The following BCM references and documents have been used:

- British Standard 25999-2: 2007 Business Continuity Management - Part 2: Specifications.
- US Standard NFPA 1600:2010, Disaster / Emergency Management and Business Continuity Programs.
- Australian/New Zealand Standard, AS/NZS 5050:2010, Managing Disruption-Related Risk.
- ISO 31000: 2009, Risk Management – Principles and Guidelines
- Singapore Standard SS540:2008 (BCM): Business Continuity Management.

Then, the information was tailored to match the nature of UAE government business. It provides the basic requirements and specifications used by internal and external parties to help entities continue performing their main / essential functions and services, comply with their organizational and contractual commitments and to protect the interests of beneficiary organizations after an emergency, crisis or disaster that hinders the entity from properly performing its functions or services. BCM requirements set out in this standard can be applied to different-sized organizations, in both public and private sectors.

The term “shall” as used in this standard refers to express mandatory requirements.

The term “should” as used in this standard refers to express guidance, which is not mandatory.

Part 1:
Specifications

1. Introduction:

1.1 Purpose of the Standard

This standard identifies the components, mechanisms and activities used to establish, implement, and continually improve business continuity management for entities in both public and private sectors.

1.2 Responsibilities

The services cabinet is responsible for ensuring compliance of all its related ministries and organizations with this standard. General Secretariat of Executive Councils and Courts of the Crown Princes of each emirate are responsible for ensuring the compliance of local organizations / entities under their jurisdiction with this standard.

1.3 Hierarchy of Plans and Authorities

The entities shall refer to the hierarchy of plans and authorities for business continuity; crisis, emergency, and incident management at the national, local, sector and entity levels as illustrated in the figure below.

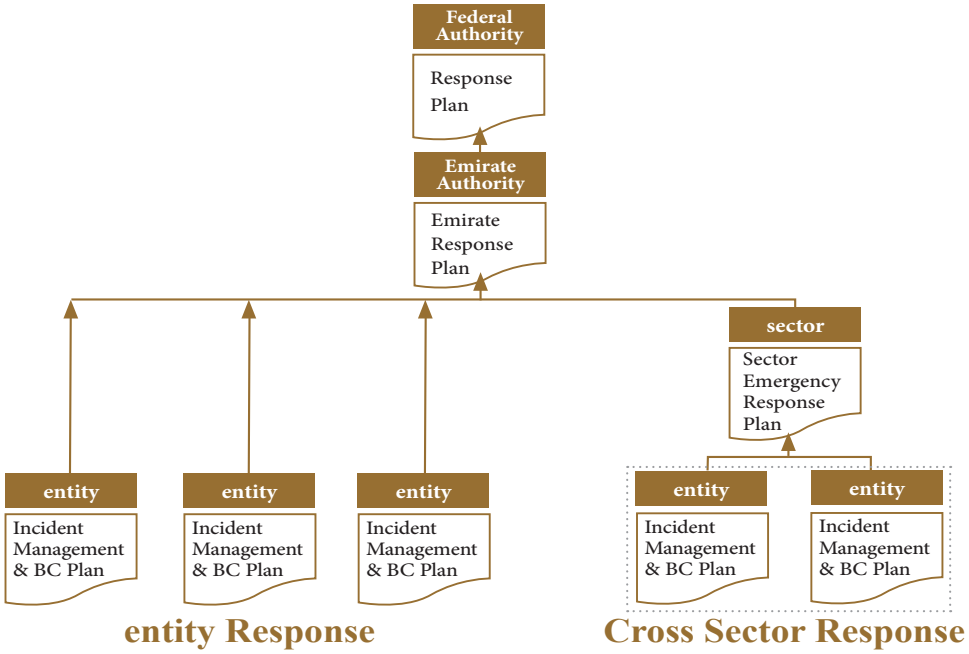


Figure 1: BCM Standard – Hierarchy of Plans & Documentation

2. Accountability Level

The entity's top management is accountable for the preparation and implementation of the BC programme. Top management might delegate responsibilities in this process to other levels of the organization. This standard, along with the related guidelines, offers the minimum requirements needed for a BC programme.

All members of the entity shall comply with the requirements of this standard and shall report any breaches, using the appropriate channels.

3. Compliance

3.1 Delegation of Authority

Bodies entrusted by the federal government of the United Arab Emirates and the local government of each emirate shall ensure the compliance of the entities under their jurisdiction with this BCM standard.

3.2 Controls set by Legislative Bodies

Legislative and licensing bodies may establish further specifications in addition to those defined in this standard to ensure community safety and security and continuity of functions and services required to promote national security. Where additional specifications are established, the entity shall comply with such specifications. However, in case of discrepancy between the specifications contained in this standard and the additional ones, such entity shall have recourse to the issuing authority of this standard for settlement.

4. Applicability

The requirements and specifications set forth in this standard are general and applicable to all UAE entities, and related bodies such as companies and key service providers to perform the functions of principal government institutions and community services.

5. Scope

5.1 Scope of the Standard

This Standard defines BCM specifications and implementation method.

A-5-1 The entity shall establish, implement, sustain, maintain, and continually improve business continuity management in accordance with the requirements of this international standard (Part 2 of this standard tackles the method of applying this standard at entities).

5.2 entity's Scope of Business Continuity Capability

5-2-1 The entity shall define the deliverables, outputs, activities, services and functions that fall within the scope of its business continuity capability.

5-2- 2 The entity's scope for business continuity shall include all activities required to maintain essential activities.

The entity shall identify all applicable legislative, regulatory and contractual requirements; and interests of stakeholders and primary partners (collectively also known as the interested parties). The entity shall also identify any internal issues, which might influence its business continuity capabilities.

6. BCM Standard Requirements

6.1 Requirements

Each UAE entity shall assume the responsibility of defining and documenting its "fit-for-purpose" business continuity capability that ensures performance of essential functions and services during emergencies, crises and disasters.

6.2 Requirements to define BC Capability:

a. To identify, analyze and document the expected risks that may cause disruption to an entity's business;

b. To identify the minimum (acceptable) level of impact on entity business;

c. To establish an ongoing mechanism; to mitigate unacceptable losses and impacts resulting from:
   - Unavailability of key staff at the entity;
   - Loss/ unavailability of main facilities at the entity;
   - Loss/ unavailability of main / essential assets and vital records;
   - Loss of access to Information and Communication Technology (ICT) systems and entity data ; and
   - Good supply and service disruption by internal and external sources in entity's supply chain.

d. When disruption of business occurs, what are the minimum services/ functions required to maintain and maximum period required to regain the capacity to perform main / essential services and functions;

e. To develop, sustain and implement response and BC plans. (Such plans should include emergency, crisis, disaster and communication management);

f. To ensure the entity has the capacity to maintain continuity of main/ essential functions and services at the pre-determined levels of

performance appropriate to the scale and impact of disruption;

g. To ensure personnel are trained to perform their BCM roles and responsibilities;

h. To conduct regular exercises to ensure the efficiency of BCM plan and staff training; and

i. To update entity's risk assessment register (log), conduct Business Impact Analysis (BIA), BCM planning assumptions, and plans in response to material changes in entity's organization, infrastructure, staff, and location of operations management.

7. BCM Documentation and Records

7.1 Required Documents

7.1.1 The entity shall maintain a documentary record of Business Continuity (BC) capability program implementation procedures.

7.1.2 entity's BC capability documents shall at least contain, and not exhaustive to, the following:

a. Concept;
b. Policy;
c. External resources;
d. Competency of personnel;
e. Business Impact Analysis (BIA);
f. Risk Assessment (RA);
g. Strategy;
h. Emergency, crisis or disaster plan;
i. BCM Plan;
j. Exercises record;
k. Review record;
l. Internal Audit;
m. Preventive and corrective actions.

7.2 Controlling BCM Documentation and Records

7.2.1 Controls shall be developed to ensure BCM documents:

a. Are easily understandable, identifiable and accessible especially in times of emergency, crisis or disaster;

b. Provide the identification needed to store, protect and easily retrieve them;

c. Are approved for compliance with the standard prior to issue;

d. Are reviewed, updated, and re-approved if need be, in addition to documenting all updates;

e. Update to date copies are available where needed; for instance, alternative sites and other points of use;
f. Identify documents received from external sources; and
g. Subject to controlled and monitored distribution and change control.

8. BC Programme Development

8.1 BC Program Development

A BC Program shall be developed in accordance with the requirements in this Standard; this shall include commitment of Top Management and ongoing test, exercise, review and development. Where an entity already has BCM Plans in place prior to the issuance of this Standard, this Standard shall be used as a scale to ensure these requirements are met or even exceeded, at the federal, local or entity levels in both public and private sectors to establish, sustain and maintain the BCM.

8.2 Top Management Commitment

8.2.1 Top Management shall ensure that the entity's BCM concept and objectives are identified.

8.2.2 The entity shall identify and provide the resources required to implement and maintain its BCM program and ensure allocation of resources required to achieve continuity of its critical activities.

8.3 Business Impact Analysis (BIA)

The entity shall define and document a method for identifying the business impact of disruptions of main / essential services / activities.

8.4 BIA Documentation

The entity shall identify and document the impact of business disruption by:

a. Identifying its core / essential functions, activities and services;
b. Identifying actions required to support main / essential functions, activities and services;
c. Identifying disruption impacts on performance of main/essential functions and services and determining how the impact increases or decreases over time;
d. Identifying the maximum tolerable period of disruption of each activity / service disruption;
e. Identifying activities / services deemed paramount to the continuity of main/essential products, functions and services;
f. Classifying main / essential activities and services according to their recoverability priority, as per the BIA;

g. Identifying internal and external bodies, which an entity relies on for continual performance of main / essential activities and services, including suppliers and service providers;
h. Reviewing the current emergency plans of the entity (if any);
i. Reviewing all emergency plans of suppliers and companies, to ensure their capability to continue providing their services and products in times of emergency, crisis or disaster.
j. Identifying the indispensable resources for each activity, function or service to ensure business continuity; and
k. Establishing a recovery time objective (RTO) to regain ability to resume main activities within their Maximum Tolerable Period of Disruption (MTPD).

8.5 Risk Assessment

The entity shall conduct a risk assessment to identify, analyze and evaluate the business continuity risks it faces. The risk assessment process should be carried out by a well-defined and approved method and the risk assessment shall be updated in regular intervals, and if significant changes occur.
The entity shall:

- Identify the risks that can disrupt or halt performance of main/essential activities and services;
- Analyze the risks by
- Analyze the impact of underlying risk factors which result in business disruption; and
- Take account of interdependencies related to the performance of critical / essential activities and services, upon impact identification;
- Evaluate the risks against predefined evaluation criteria.
- Analyze its vulnerability to risks by:
  a. Identifying incidents resulting in business disruption (such as risks, threats, etc.).
  b. Assessing the direct and indirect impact these incidents could have on the entity's day-to-day operations, performance of its main / essential activities and potential increase in demand for other services.
  c. Documenting and prioritizing its risks in accordance with risk assessment.
  d. Identifying and controlling vulnerabilities on an ongoing basis.

8.6 Risk Management Strategy

The entity shall implement and document risk management to handle the risks to its main / essential activities and services, as per its acceptable level of risk.

8.6.1 Risk handling strategies should be identified and tailored to:

a. Reduce the possibility of a disruption;
b. Shorten the period of disruption; and
c. Mitigate the impact of disruption on the entity's / main / essential activities and services.

8.6.2 The entity / organization shall present risk-handling recommendations to Top Management for review and approval.

8.7 Business Continuity Management Strategy

The entity Top Management shall develop and approve BCM strategies, to be able to continue performing its main / essential activities and services following a business disruption, due to such risks which could not be removed or mitigated to acceptable levels.

8.8 Business Continuity Management Plan

The entity shall develop BCM plans in support of its strategies, as follows:

8.8.1 The entity shall have documented plans detailing its business disruption response, emergency and crisis management and recovery methods, to sustain continuity of its main / essential activities and services at the predetermined performance levels following a business disruption.

8.8.2 Each plan shall:

a. Have a defined purpose and scope;
b. Be made available to all personnel that needs to be aware of it, and to personnel with specific roles and responsibilities for review and update;
c. Be consistent with the BCM strategy and with plans, capabilities and requirements of external stakeholders; and
d. Be accessible to and understood by stakeholders upon implementation.

8.8.3 All plans shall contain:

a. Identified lines of communications;
b. Key obligations and reference information;
c. Defined roles and responsibilities of personnel and teams during and following an incident;

d. Identification of people who have the authority to use each plan under any given circumstances;
e. Criteria for invoking the plan and the method whereby the plan is invoked;
f. Statement of main and alternative meeting and work locations;
g. Contact details of agencies, Entities and beneficiary suppliers, which are paramount to the management of emergency, crisis or disaster and business continuity management;
h. Recovery procedures to be followed to return to normal after the emergency or disaster have struck.
i. Emergency and crisis response guidelines, taking into account the following:
    - Welfare of individuals
    - Prevention of further loss or unavailability of main / essential activities and services
    - Impact of disruption on main / essential activities and services
    - Strategic and operational options for disruption response
j. Clear-cut communication mechanism to enable personnel and mass media to communicate to get better acquainted with the emergency, crisis or disaster developments.
k. Emergency, crisis or disaster management guidelines including steps to:
    - Handle emergency and crisis developments; and
    - Issue prompt recovery instructions in order to continue performing main / essential activities and services.
    - Details on how and under what circumstances would the entity communicate with employees and their relatives, key stakeholders and emergency contacts;
    - A method for recording information about the emergency, crisis or disaster, as well as the actions taken and decisions made;
    - List of actions and obligations that need to be performed;
    - List of the resources required for recovery
    - Prioritized objectives in terms of main / essential activities and services to be recovered, recovery timescale and recovery levels needed for each main activity.
    - "Standing down" once incident is over and returning to normal duties.

8.9 Awareness and Training

The entity shall ensure that a training and awareness programme is developed and implemented that effectively supports the BCM objectives.

8.9.1 Staff Awareness
The entity shall ensure BCM integration into its day-to-day business processes, through an ongoing training and awareness programme which shall be documented. The Staff Awareness Programme shall:

a. Establish the foundation for evaluating its effectiveness;
b. Spread BC capability and awareness;
c. Communicate implications of not conforming to BCM requirements;
d. Ensure continual improvement of BCM; and
e. Ensure personnel are aware of their roles and responsibilities in BCM programme.

8.9.2 Training
The entity shall ensure that the training provided for personnel and teams matches their roles and responsibilities, including but not limited to, response, continuity, sustainability and continual development.

8.9.3 Training Records
The entity shall document and maintain BCM training records.

8.9.4 Spread BCM awareness among external stakeholders.
The entity shall notify its suppliers and beneficiaries of their responsibilities to meet the requirements to achieve BC and communicate BC documents, as appropriate.

8.10 Tests and Exercises
The entity shall conduct tests and exercises to ensure the BC plans remain fit-for-purpose and effective, and shall maintain a rolling one year 'Test and Exercise Plan'.

8.10.1 Tests
Tests shall be conducted to assess readiness, usability and adequacy of the tools, technology, facilities, and infrastructure required to implement the entity's BCM plans. the tests shall produce reports and these reports shall be reviewed and corrective action takes, when necessary.

8.10.2 Exercises
Exercises shall be conducted to verify that the personnel and processes required to implement the entity's BC plans meet their objectives established in the BIA. The exercises shall fulfill the following requirements:

a. Ensure exercises are carried out periodically and if changes occur that affect main / essential activities and services;
b. Conduct a range of exercises that taken together validate the whole of the entity's Business Continuity capability and focus on highest level risks identified in Section 8.5.;
c. Plan exercises so that the business disruption occurring as a direct result of such exercises is minimized;
d. Provide a standardized unified procedure methodology and interact with other entities / organizations in a unified framework to the extent possible;
e. Define the aims and objectives of each exercise;
f. Write a report on such exercise detailing the outcomes, feedback and suggestions including required actions and remedy plan;
g. Carry out a post-exercise review, to assess the achieved objectives of the exercise and extract lessons learnt for the purpose of development.

NCEMA will perform periodic exercises at the national level, to ensure alignment of plans within all UAE entities in order to ensure mutual cooperation and coordination among such entities.

8.11 BCM Continual Improvement

8.11.1 Requirements

The entity shall ensure BCM objectives are met through periodic review, including self-assessment, and continual improvement of its plans, performance and documentation.

8.11.2 Methodology

Periodic review and continual improvement shall be performed through:

a. Regular review of changes to the business and risks that can result in business disruption, as well as the impact of such disruption, and the increase or decrease in risk appetite;
b. Reviewing and examining risk treatment and business continuity strategies; and
c. Approving response, incident management, communication, continuity and recovery plan(s) tailored to achieve the entity's BCM objectives.

8.11.3 Results

The review results shall be documented by the entity's Business Continuity officer, and then reported to the Top Management.

8.11.4 Inconsistency
The entity shall address its BC capability's in consistency with this Standard, through preventive and corrective actions.

8.11.5 Preventive and Corrective Actions
Preventive and corrective actions shall be aligned with the Business Continuity Policy and BCM objectives at the acceptable level of risk, as may be determined by Top Management.

8.11.5.1 Preventive Actions:
a. The priority of preventive actions shall be based on the results of the entity's risk assessment and BIA.
b. Preventive actions should be commensurate with the potential impact of the emergency, crisis or disaster.
c. The preventive actions standard should define the necessary requirements.

8.11.5.2 Corrective Actions:
The entity shall take required action to eliminate the causes of non-conformity with the Business Continuity Management policies, procedures and plans and prevent their recurrence. The procedures shall explain and document corrective actions, defining points and causes of non-conformity and recording all action taken.

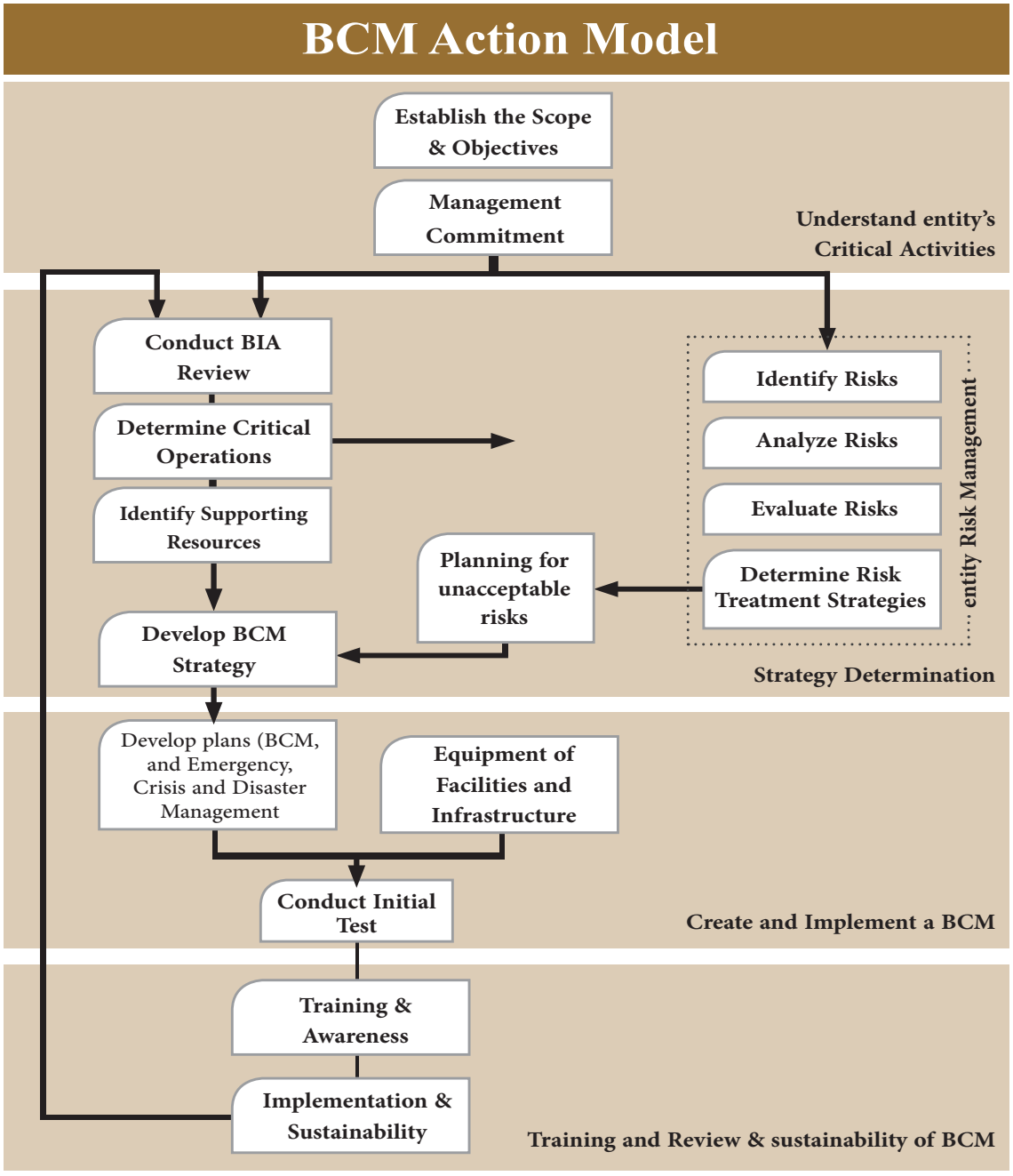


Figure 2: BC Model

8.11.6 Conformity and Certification

The entity should ascertain conformity and certification to this standard. This can be through a self-assessment or third party assessment or third party certification.

In due course, NCEMA will develop a process for third party certification as well as identify the agency that will be authorized to do the third party certification of this standard.

8.11.7 Compliance and Internal Audit

The entity shall plan, develop, implement and maintain a programme to audit its BCM.

8.11.7.1 Annual Internal Audit

The entity shall conduct a complete annual internal audit of its BCM. This audit shall cover all requirements of this Standard, and selected elements of the Guidance.

8.11.7.2 Internal Audit Program

The Internal Audit Program should address all aspects of the entity's BCM capability building programme.

8.11.7.3 Internal Audit procedures

The entity shall develop procedures to implement its Internal Audit Programme which:

a. Identifies the responsibilities, competencies and requirements for planning and conducting audits, reporting results and maintaining related records; and
b. Identifies audit criteria: scope, frequency and methods.

8.11.7.4 Internal Audit Report

The results of the entity's Internal Audit shall be documented in an Audit Report which shall:

a. Contain audit results and recommendations for improvement.
b. Be submitted to Top Management for review.

The entity shall ensure that corrective action is taken for any non-conformities that have been identified during the internal audit, and that the findings are closed as planned.

9. BCM Measurement and Evaluation

9.1 Annual BCM Review

In order to continually improve its BCM capability, the entity should, at least once per year, review its:

a. Policy and objectives;
b. Plans;
c. Planning assumptions;
d. Allocation of resources;
e. Exercise results;
f. Audit results; and
g. Preventive and Corrective Actions.

9.2 Review of Key Suppliers

The entity shall:

9.2.1 Ensure its key suppliers are sufficiently capable to meet the identified BIA requirements.

9.2.2 Assess supplier capability through joint tests and exercises with the entity, or through entity review of the extent of supplier's compliance with this Standard.

9.3 Review of Third Parties

Where necessary, the entity shall ask its third part service providers to periodically test at least those operations related to the entity and to provide the entity with the test reports.

9.4 Post-emergency, Crisis, Disaster Review

A post-incident review and key lessons learned log shall be retained resulting in the activation of emergency, crisis or disaster Management plan or Business Continuity Plan.

9.5 Annual BCM Evaluation Report

The entity shall summarize its BCM activities in an annual report. This report shall:

a. Record and evaluate the capability demonstrated during real exercises, emergencies, crises or disasters against continuity and performance objectives set out in the BIA;
b. Identify actions required to ensure BCM recovery, and performance objectives in the BIA are met; and
c. Identify actions to ensure that entity meets the Performance Objectives set by the government.

10. Management Review

10.1 Management Review of BC Program

Management shall periodically or when significant changes occur, review the entity's BC capability to ensure it remains fit-for-purpose and continues to meet BCM objectives. The Management Review shall be carried out at least once per year.

10.2 Documentation of the Management Review

The results of the management review shall be clearly documented and records shall be maintained.

10.3 Points to be accessed during management review

The entity shall ensure that the following points are addressed in the management review:

a. Results of BCM audits, post emergency, crisis or disaster reviews, and exercise results;
b. BCM status of key suppliers and outsource partners, as available;
c. Level of remaining and acceptable risks;
d. Inadequately managed risks, including those identified in the entity's previous risk assessment;
e. Internal or external changes likely to affect the entity's BCM capability;
f. Results of exercises, tests and self-assessments;
g. Accomplishments of training and awareness programs;
h. Follow-up procedures based on previous management reviews; and
i. Proposed recommendations for development of the entity's BCM capability.

10.4 Management Review Outcome

Management review shall include the following decisions and recommendations to address:

a. Deficiencies in the entity's BCM capability;
b. Enhance the effectiveness of entity's BCM capability;
c. Change the entity's:
    - Strategies and procedures to respond to internal or external incidents likely to impact its BC capability;
    - Need for resources required for BCM;
    - Budget of BCM program; and
    - Method of funding the BCM program.

Part 2:
Guide

A.1 Introduction

A.1.1 Purpose

This section of the document provides a common set of guidelines that can be used to develop and implement BCM by all entities. This document is intended to help:

- Understand business objectives and identify main / essential business activities;
- Examine the extent of risk impact on business disruption;
- Analyze business disruption impact on main/ essential activities;
- Make informed decisions about how to ensure continuity of activity;
- Develop entity's BC capability to perform main/ essential activities during and after an emergency, crisis and disaster; and
- Develop an integrated and coordinated set of plans to achieve a BCM capability.

A.1.2 Responsibilities

NCEMA is committed to setting the BCM standard and provide technical advice to implement such standard.

A.1.3 Hierarchy of Plans and Authorities

BCM plans should be developed to ensure continuity of main/essential activities.

At the Federal Government level, the entity puts an internal emergency response plan in place, to be implemented by a national crisis and emergency management team.

Within each Emirate, there will be an Internal Crisis and Emergency Response Plan that will be implemented by local crisis and emergency management teams.

Where a local or federal government has established an Authority to oversee activities in a particular sector, there shall be a Crisis and Emergency Response Plan tailored to such Sector and implemented by the leading body in it. For instance, the Telecommunications Regulatory Authority is responsible for developing a Telecom Business Continuity plan in the UAE.

The foundation of all business continuity depends on the individual entities and organizations in government and the private sector. Each entity is held responsible for developing its own crisis and emergency management and BC plans.

A.2 Accountability Levels

Escalation of Incident Level
In case of increased occurrence of emergencies or business disruptions in one or many entities, it may be necessary to escalate this issue to higher-level authorities, and then additional resources needed to manage and respond to such events can be called in.

The points of contact, escalation procedures and escalation level should be documented in emergency, and crisis management plans.

A.3 Compliance

A.3.1 Delegation of Authority
Higher authorities are responsible for appointing the bodies in charge of overseeing the entities' compliance with this Standard.

A.3.2 Controls Set by Legislative Bodies
At some entities, such as Financial Services, Aviation, Telecommunications, and Healthcare entities, a regulatory agency may have authority over the entities that operate under its supervision. In this case, the regulatory agency may set its own requirements for its related entities to develop crisis and emergency management, and business continuity capability.

These requirements have been developed in accordance with crisis, emergency and business continuity management procedures and principles that are applicable to various entities.
This Standard provides the minimum BCM development requirements. Where a legislative body establishes requirements beyond those contained in this Standard, its related entity shall comply with the Regulatory Agency's requirements.

In case of discrepancy between the requirements of this Standard and the requirements of the regulatory agency, the entity should send a written request to the regulatory agency and keep a copy of the agency's reply. The regulatory agency should then inform the Supreme Council for National Security of the conflict and the recommendation it has made to resolve the conflict.

A.4 Applicability
Pursuant to this Standard, the entity should identify its main / essential

activities as well as the business units, departments and sections where such activities are performed. In addition, the entity should identify its related bodies such as third-party suppliers, service providers and partners that provide goods and services needed to perform these activities.

A.5 Scope

A.5.1 Scope of the Standard

A.5.2 Scope of the entity's BC capability

A.5.2.1 Locations, facilities, products, functions and services within the scope

Locations, facilities, products, functions and services may not be wholly included in an entity's BCM program.

The definition of in scope and out-of-scope elements with respect to the entity's BCM program is based on a decision by Top Management about the business activities which are deemed as critical / essential in supporting the entity's business objectives. With this in mind, in-scope locations, facilities, products, activities and services can thus be identified. It is also based on the actions taken by an entity to identify and remedy the potential causes of business disruption i.e. risk treatments it has in place.

The entity should keep record of in scope activities, locations, products and services etc. along with justification for inclusion and exclusion.
(For more details, see Section 8.5 on Risk Assessment, Section 8.6 on Risk Strategy, and Section 8.7 on BC Strategy)

A.5.2.2 Define and allocate the resources required to:

a) To initiate its BC program development, an entity should identify the employees, facilities, equipment, and supplies needed by the teams to develop, update and implement its BC program. The entity should set a budget and develop a project plan to implement the program in addition to establishing goals and performance objectives for the teams involved.

(See 'BC Toolkit 1 – Templates' for a BC Project Plan Template and 'BC Toolkit 2 – Examples' for a sample plan).

b) Primary objectives of entity's day-to-day activities as per its regulatory obligations.

c) When conducting risk study, there will be some unavoidable acceptable risks and unacceptable risks. Thus, such risks should be clarified in the program, as they constitute the greatest threat to the entity.
d) All contractual obligations with suppliers, service providers or others should be set along with other legislative obligations, in accordance with the laws and regulations and any regulatory obligations.
e) All partners and bodies beneficiating from the entity's services should be taken into account and a list of their names should be created.

A.6 BCM Requirements

A.6.1 Requirements

The primary purpose of a BCM program is to enable the entity to promptly and effectively respond to business disruption and maintain continuity of its main / essential activities.

This is achieved by implementing the BCM program and developing the policy, plans, and capabilities that will enable it to achieve its emergency and crisis response objectives, ensure business continuity and recovery, as specified in its BIA. (For more details, see section 8.4 on Business Impact Analysis "BIA" Documentation).

A.6.2 Requirements needed to identify "the necessary BCM Capability" can be summed up as follows

A.6.2.A Identify, analyze and document potential risks

The risk assessment process is initiated by identifying threats which affect the performance of main / essential activities required to accomplish an entity's business objectives. This process can be time-consuming and involves developing a list of all threats, or can be carried out by making a list of the events most likely to disrupt operations and then the risk level of each event is assessed. For more details, see section 8.5 on Risk Assessment).

A.6.2.B Determine the minimum (acceptable) level of impact on entity business.

By identifying impact areas and determining the level of impact within each area, the entity can build a Table sometimes called "Impact Severity index" for emergency, crisis and disaster management.

Impacts: Emergency, crisis or disaster could impact the entity in a number of areas including:

- Personnel – unavailability or inability to perform the work.
- Financial Status – losses or costs threatening the financial status.

- Day-to-day Operation – inability to perform day-to-day activities.
- Reputation – damage to the entity's reputation or loss of confidence in its leadership.
- Compliance with contractual, legal and regulatory obligations - by resulting in a failure to comply with the law, the terms of entity's license, contracts and agreements.

Levels: One way to measure impact is to use numeric values, such as Dirham value to get acquainted with the financial impact. Another way is to use qualitative values such as High, Medium, and Low to measure the level of impact on entity's Reputation.

Another method involves a combination of quantitative and qualitative values, as in the example below where a five-point scale is used, with 1 being minimal impact and 5 being severe using the following criteria:

- Minimal temporary disruption: no impact on business operations or main/ essential activities
- Low temporary disruption: short-term impact on business operations or main / essential activities
- Medium: short-term or ongoing disruption, short-term impact on business operations, and inability to perform main / essential activities
- High short-term, long-term or ongoing disruption, and impact on business operations, unable to perform most of the critical / essential activities
- Severe long-term or ongoing disruption, and impact on business operations and inability to perform all main / essential activities
- Within the framework of its BC strategy, Top Management needs to identify the acceptable and unacceptable levels of impact. Top Management's identification of unacceptable levels of impact defines the entity's Risk appetite or tolerance.

A.6.2.C Develop an ongoing mechanism to reduce unacceptable losses and impacts

Those reporting to Top Management are responsible for analyzing the risks that could result in unacceptable loss and determining whether risk handling actions are required to reduce loss.

A (1) A number of workers should be qualified to perform important and critical functions within the entity, to be able to replace absent workers for any reason whatsoever.

A (2) Agreements should be concluded and alternative facilities for most significant facility should be prepared such as the entity's primary operations room. The alternative operations room should be placed in a remote location to be properly used when disruption occurs in the primary location.

A (3) Backup copies of entity's significant records should be maintained and a mechanism should be developed to compensate any of the primary properties or assets.

A (4) A BC plan should be available for information assessment as this requires a number of procedures of information and communications assessment.

A (5) Alternative sources of third-party suppliers should be found and agreements or MOUs should be concluded with such bodies to be used where key suppliers fail to fulfill their obligations towards the entity, in order to ensure continuity of supply chain and disruption would not impact entity's activities.

A.6.2.D Identify recovery objectives of main/ essential activities

The maximum timeframe during which the entity should recover the minimum limit required to deliver main / essential activities shall be set, by establishing a timeframe showing the service and time required for recovery until it reaches the level that enables the entity to achieve the recovery objectives predetermined in the plan. This information can be obtained through BIA.

A.6.2.E Develop, sustain and implement response and BC plans pertaining to main and essential activities.

The entity's Incident Management Plan should provide Top Management and Incident Management Team with contact information, assessment criteria, escalation protocols and key action plans needed to provide strategic direction and co-ordination during an incident to manage its response, continuity, and recovery.
This is intended to:

- Ensure the safety of personnel affected by emergencies, crises and disasters and plan response;
- Assess disruption impact;
- Co-ordinate continuity and recovery efforts of BC teams;

- Provide coordinated and managed communications to internal and external stakeholders, including media; and
- Protect the entity's assets and resources from future damage and losses.
-

(See 'BC Toolkit 1 – Templates' for a BC Plan Template and 'BC Toolkit 2 – Examples' for a sample plan).

The entity's Business Continuity Plan provides instruction and guidance needed for business and support staff, so as to perform main/essential activities at an alternative work site, or in diminished capacity at the primary work site.

(See 'BC Toolkit 1 – Templates' for a BC Plan Template and 'BC Toolkit 2 – Examples' for a sample plan).

The entity's Recovery Plan provides instruction and guidance to return to normal duties after an emergency, crisis or disaster.

An Independent Information Technology Disaster Recovery (ITDR) plan should be developed to support continuity of the entity's main activities and those pertaining to IT infrastructure. The ITDR Plan provides instruction and guidance to Information Technology (IT) personnel to regain access to and use information, data, and communications systems required to perform the entity's main activities. The ITDR Plan is developed by the IT Department, or its related vendors to maintain IT and telecommunications systems. (For more details, see Sections 8.8.2 and 8.8.3)

A.6.2.F Ensure capability of continuity and sustainability of main / essential services and functions

Plans should be developed that allow a certain level of response that suits the severity of emergency, crisis or disaster.

Rather than start with a full invocation at the outset of every incident, the entity should activate its incident management teams to a level appropriate to the scale of the event and the amount of information available regarding the impact of the emergency, crisis and disaster.

To prepare for situations that may result in lack of resources needed to respond to a larger emergency, crisis or disaster, the entity should identify

additional resources that can be called on to provide aid and support. This may include the activation of teams from other Entities to assist in response, including requesting additional help from local authorities, or escalation of incident management to teams outside the area of impact.

As the impact of an emergency or crisis or disaster becomes more severe, it can require more resources for initial response than for normal operations. In some cases, the need for support from Human Resources, IT and Building Services may be two or three times greater than it is normally. At the same time, there will be a decrease in certain levels of performance, or "turnaround", for activities most impacted by the disruption.

In this case, the department shall prioritize its tasks and adjust its expectations of what work will be completed and how long it will take to complete such work as long as it is operating in 'crisis mode'.

The Business Impact Analysis can be used to adjust expectations for the level of performance, time to recover, and the resources required to restore continuity of operations. Until such requirements are met, the entity will need to prioritize allocation of its limited resources and adjust performance expectations across its business units, departments and operations. (For more details, see section 8.8 on BCM plan).

A.6.2.G Ensure personnel are trained to perform their BCM roles

A BC program requires that all personnel assigned roles and responsibilities in developing and implementing the program as well as conducting the response, continuity and recovery from an emergency, crisis and disaster are trained to acquire the required skills to perform their assigned roles.

(See 'BC Toolkit 1 – Templates for a Training Record Template' and 'BC Toolkit 2 – Examples' for a sample training plan).

(See 'BC Toolkit 3 – Training' for a recommended training program for each role and recommended training providers)

A.6.2.H Conduct regular exercises to ensure the efficiency of BC capability plan and train staff on such tasks;

Exercises are essential to ensure that personnel entrusted with roles and

responsibilities in BC program are able to perform such roles in a controlled training environment.

Exercises also provide the opportunity to determine whether the contents of an entity's BC plans are valid, the procedures contained in such plans are up-to-date and consistent with the training provided to such employees in charge of implementing these plans. These exercises should be carried out regularly and at different levels.

A.6.2.I Update entity's risk assessment register, BIA, BCM planning assumptions, and plans in response to material changes in entity organization, infrastructure, personnel, processes and location of operation.

Major changes can occur when changes are applied to:
- Strategic objectives;
- Size of the organization;
- Top management;
- Key personnel;
- Services;
- Activities that require performance of such services;
- Locations;
- Tools and equipment used to perform these activities (including IT); and
- Supplies, suppliers, and service providers.

When such changes occur, the entity should consider reviewing its Risk Assessment, BIA and BC Strategy to determine whether they need to be revised and updated.

Where changes result from updating or amending the entity's BC or Incident Management plans, the entity may need to ensure objective achievement, by conducting an exercise that may not be programmed.

A.7 BCM Documentation and Records

A.7.1 Required Documentation

A.7.1.1 Details provided in an entity's BC documentation should be sufficient to describe BCM process, identify the components, and indicate how the components integrate.

Such documentation should be prepared in an understandable and unified way, and should focus on providing and maintaining the effectiveness of its preparedness and response to business continuity. Thus, such documentation shall be as simple as possible.

The extent of BC program documentation can vary from one entity to another based on the size and type of the entity, its nature of work, variety of its services and activities as well as the personnel experience in emergency, crisis and BC management.

A.7.1.2. BCM program documentation should at least include the following instruments:

a) BCM Concept and objectives including limitations;
b) BCM policy;
c) Capability of providing external resources;
d) Records pertaining to the extent of competency of personnel involved in BCM program and the relevant training records;
e) Business Impact Analysis based on entity's risk record;
f) Risk assessment register;
g) BCM strategy;
h) Emergency, crisis or disaster response plan;
i) BCM plan and emergency, crisis or disaster management plan;
j) Exercise reviews record and BCM test results;
k) Review record and continuous development of BCM program;
l) Internal Audit operations with respect to the BCM program;
m) Record of preventive and corrective actions and lessons learnt from exercises;
n) Corrective and preventive actions (for nonconformities found during audits) plan; and
o) Management review annual record.

A BCM Procedures Manual may be created to have all processes (methods)

and associated templates (where necessary). These processes should be executed at a defined frequency. The results of the execution of each process should be documented and published to relevant interested parties. These results should be used in managing the entity's BC.

(See 'BC Toolkit 1 – Templates' and 'BC Toolkit 2 – Examples').

To properly utilize, maintain and extract documents, the following points should be taken into account:

a) Translate these documents into more than one language based on the entity's nature and nationalities of its personnel especially those involved in implementing entity's plan or mission or entrusted with specific roles and responsibilities. At all events, such copies shall be issued in both Arabic and English language.
b) Maintain these documents so that they can be easily accessed by personnel when needed, distinctive color is preferred.
c) Ensure documents conformity with the Standard by the entity's Steering Committee.
d) Conduct ongoing review of all documents. Should any amendment, addition or cancellation be made to the documentation of this Standard, they should be reapproved by the Steering Committee.
e) Provide copies of the plan or instructions required in the plan or place bulletin boards in main and alternative locations (if any), as well as in all entity's branches, in addition to making all important and key documentation available.
f) If documentation or information from external sources are used, such sources should be determined and recognized in all used documentation.
g) A documentation control and distribution system should be created to ensure that all copies retained in all locations are properly updated.

A.8 Developing BC Program

A.8.1 In addition to the first part of this Standard, a member of Top Management, known as the BC Program MR (Management Repsentetive) is appointed in many cases to be fully responsible for the Program. This person should enjoy leadership and proper powers and authorities to ensure the entity's BC Program is established, maintained, and implemented effectively.

In many Entities, this person will be known as the Business Continuity

Manager. Depending on the size of the entity, it may be a full or part-time duty. To emphasize the importance of duties and responsibilities associated with the BC program, the position should have specific BC elements incorporated into the job description, including fulfillment of duties taken into consideration as part of the annual job performance review. The entity's Internal Audit function should include the review of the assignment of BC program positions and duties as part of its annual program assessment.

Staff assigned positions and duties or roles and responsibilities in the BC program should be provided with the required awareness, education, and training to fulfill their responsibilities in maintaining and operating the entity's BC program.

Validation of the effectiveness of the entity's Business Continuity capability should be provided through training and tests, at least annually.
(See Section 8.10 for further details).

A.8.2 Top Management Engagement
The Program manager should ensure the concept and objectives of the entity's BC plan are clearly defined in the Project Management Document, which is sometimes known as a BC Project Document.

A.8.2.1 the Project Management Document should include the project scope, resource plan to identify the range of staff, facilities, equipment and material needed to develop the BC capability program, to identify the sequence of activity and timeframes required to develop the program.

The Project Scope Document should identify:
- Agreed-upon objectives and business priorities;
- The deliverables required during the project and delivery times of primary and final products;
- All standards or regulatory requirements to be met;
- Any assumptions whereby risk or impact statements can be provided;
- Locations and / or job functions to be included in or excluded from the BC capability program;
- The Risk Appetite (level of risk that requires risk handling or response);
- All specific risks to the success of the project;
- The organizational structure of the entity's BCM program (roles and responsibilities)

An assessment should be conducted to compare the entity's current capability against the standard- required level or enhanced requirements of the regulatory agency. The results of such assessment should be incorporated into a Statement of Applicability (SoA) Report and submitted to Top Management to highlight the gaps to be addressed, so as to improve the entity's BC capability. The capability assessment and SOA Report should be integrated with the entity's annual BC capability performance review.

(See 'BC Toolkit 1 – Templates' to review the Project Scope Document and Statement of Applicability (SoA)).

A.8.2.2 In addition to providing resources for the development of the entity's BC capability program, Top Management should also provide the resources required to ensure the validity of the program. This should include:

1. Appointing a person or team to manage the BCM;
2. Defining the scope of the management process and BCM program.
3. The person appointed to run the BCM program should:
    - Develop and approve a documented process for planning and developing the BC program.
    - Determine and document the approach to implement each stage of the BC program.
    - Ensure appropriate levels of training are provided to the team responsible for implementing the BC program.
    - Train staff of operational departments at main locations to:
    - Act as a point of contact for BCM program activities which affect the department or location;
    - Assist the department in identifying the impact of process changes on the entity's BC capability;
    - Update the entity's BC Plan or sub-plans, to ensure they remain valid and consistent with the changes that have impacted the entity's BC capability;
    - Assist or manage the department or location's response and recovery from main / essential activities in the event of a business disruption.

The entity's BC program should include all the tasks required to implement and maintain its BC capability and such tasks are to be entrusted to qualified individuals who are able to perform such tasks. Also such tasks shall be monitored to ensure they are properly fulfilled in such a way as to achieve entity's BC objectives.

Additional groups may be formed to assist in BCM development. These include:

BCM Program Team or Steering Committee – a strategic management group composed of executives, officers or section heads, whose function is to provide advice, guidance and management supervision.

Incident Management Team – a high-caliber tactical team composed of representatives from all teams involved in incident response, whose function is to resolve coordination issues and assist in the management of incident.

Business Response and Continuity Teams – the operational teams are composed of representatives from each department involved in response and recovery, whose function is to develop and implement the BC Plans for a department or location.

The Policy should be defined at this stage, bearing in mind it can be enhanced later as the program develops.

A.8.3 Business Impact Analysis (BIA)

Training courses are held to qualify BCM program staff to perform their entity's BIA. Also, specialized centers can be capitalized on to perform such a task in favor of the entity. The significance of this BIA is generally shown below.

BIA is the foundation upon which the entity's BC program is built. It identifies and measures business disruption impact or disruption of some or all activities. It also provides data required to determine appropriate BC strategies.

BIA can be used to identify the time scale and extent of disruption at strategic, tactical and operational levels. For example:
Strategic: the loss of ability to deliver a product or service can be used to assist in deciding the scope of the entity's BC program.

Tactical: An interruption to the internal and external activities that would disrupt the delivery of products and services can be used to provide information relevant to the selection of appropriate continuity options and the determination of resources needed to implement these options.

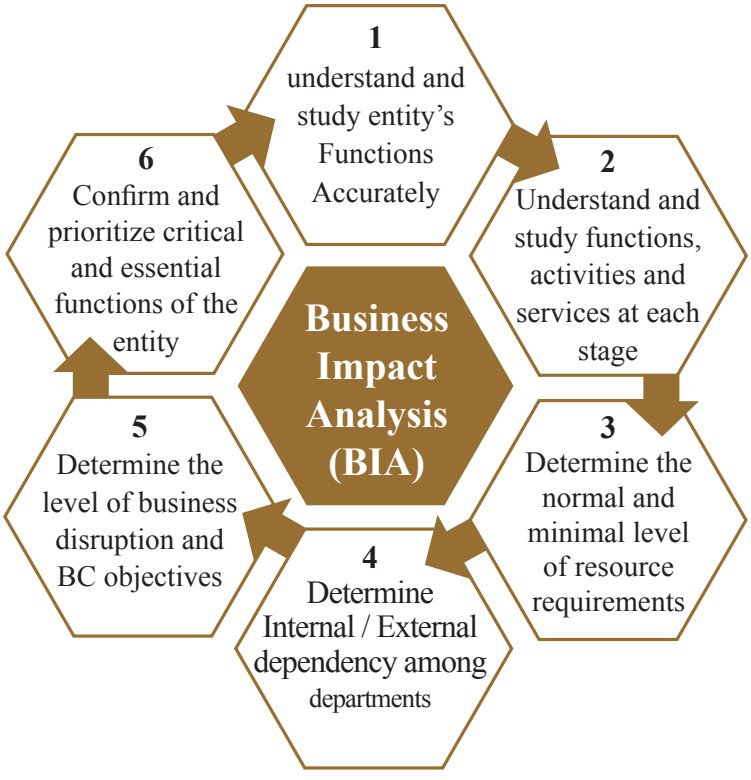
Operational: A disruption of a business department's activities can be used to assist in developing detailed response and recovery plans to meet the entity's BC capability performance objectives.

The Top Management should determine the essential products and services. In the beginning of the program, instead of including all products and services, the BIA can be performed only with respect to the products and services already classified as essential.

BIA should be conducted for all processes/ activities. One of the outcomes from BIA is RTO, which helps in prioritisation of processes/ activities and identification of main/ essential activities to focus upon during disasters/ emergencies/ crises.

BIA is also used to determine the time frames whereby essential products and services need to be restored, the assets (facilities, employees, systems and materials) that are required to produce these products and services, and the levels of performance required to achieve the entity's recovery objectives.

BIA follows the cycle of activity illustrated in the figure below:



There are several methods of conducting the BIA, including:
- Person-to-person interviews and meetings
- Opinion polls or specialized questionnaires
- Software tools or packages

Once the BIA is complete, the results are used to define recovery and continuity strategies and provide input to develop BC Plans.

Any major change in the processes used to produce an entity's critical products and services should trigger a re-review of the BIA to determine whether information in the BIA shall be updated.

BIA should be reviewed at least once a year to ensure its validity and apply the necessary changes where necessary.

(See 'BC Toolkit 1 – Templates' for a BIA Template and 'BC Toolkit 2 – Examples' for a sample of BIA).

A.8.4 BIA Documentation

It is paramount to have a clear understanding of the department-level functions, and how such functions would be impacted by a disruption. In some cases, the time-scale used to measure disruption is measured at intervals of minutes or hours, e.g hospitals and banks would be highly affected in terms of electrical power supply to the Intensive Care Unit or ATM machines. In other cases, the time scale may be measured in days or weeks with a low impact. A common time scale for measuring disruption and impact should be defined, in consultation with Top Management prior to commencing the BIA.

Business disruption impact shall be measured in terms of entity-related damage, losses, or disruption as follows:
- Operations;
- Financial Status;
- Reputation;
- Contractual obligations and commitments;
- Legal and regulatory compliance requirements.

To accurately determine the impact or its acceptable extent, the entity should clearly identify its required levels of service it needs to maintain, whether

upon suspension of such levels of service in a disaster, or the number of recovery times of service, and the penalties imposed if it fails to do so.

This should include a review of entity's:
- Service Level Agreements
- Operating Level Agreements
- Contracts
- Insurance Coverage

The impacts identified in the BIA are combined to produce a rating that provides an overall assessment of the disruption of each activity; such as the severe impact after five days or low impact after three weeks. These ratings are used to classify and categorize activities and establish recovery priorities.

When it comes to the activities which are based on IT systems and data, data loss impact between the time of disruption and time of last usable backup copy retention shall also be reviewed. This would help identify the entity's current capabilities, or the capabilities it should enjoy, to ensure continuity of performance of main/essential activities, using manual processes or workarounds involving the use of other technology tools when the system is down.

BIA also identifies the requirements for the buildings, work areas, personnel, computer systems, software applications, tools, equipment, electronic or hardcopy data, documentation, products, supplies or services provided by internal or external sources that are essential for continuity of its main / essential activities.

In conducting BIA, a common impact assessment approach is employed using a worst-case scenario. The rationale behind this is that an entity which is able to regain continuity at the most critical times would also be able to regain continuity at times when impact is less critical.

Delivery of the entity's main/essential products and services should not be disrupted by the failure of a third-party which either supplies these products and services to the entity or supplies them directly to customers on the entity's behalf.

If product or service delivery is wholly or partially outsourced, the entity should remain responsible for maintaining continuity of delivery of such

products and services to its customers. Entities that undertake to provide their facilities or services to third-party suppliers should assist such suppliers in developing and maintaining their Business Continuity capability.

Entities can do so by setting in the BIA, the suppliers' requirements in order to meet the entity's recovery objectives. These requirements should then be incorporated into contractual agreements between the entity and its suppliers.

It is important that the BCM Policy and BIA require a review of outsourced activities because stakeholders will assume that the entity is aware of its dependency on third-parties which perform activities, that it has made an informed choice about such third parties, and that it has taken appropriate measures to make sure the third parties are able to properly perform their duties, so as to maintain continuity of the entity's main/ essential activities.

Suppliers should be regularly evaluated to ensure they have the internal BC capability to deliver products and services needed to meet the entity's BIA requirements and fulfill the terms of their contracts.

To put it simply, BIA provides the information needed to identify and record the entity's main/essential products, services and the activities needed to produce them; the recovery time objective (RTO) for the data, information and systems needed to continue to deliver such activities.
(See 'BC Toolkit 1 – Templates' for a BIA Template and 'BC Toolkit 2 – Examples' for a sample of BIA).

BIA documentation should include:

a) Deep understanding of entity's business including its key businesses and essential activities;
b) Identifying activities that support such business or services provided by the entity. Other alternative sources that may replace the current supporting sources can also be identified.
c) Identifying impact resulting from disruption of any of entity's functions, activities or services by identifying the activity or service and assuming their disruption for any reason whatsoever. Then, the resulting impact and the impact of all activities' disruption should be measured, assuming, for instance, that the entity building is no longer accessible because it went up in flames or any other potential emergency. Then, the extent of such impact should be measured over time whether during the first hours, days or months for the purpose of identifying the period that can be tolerated without the entity's services.

d) the Maximum Tolerable Period of disruption "MTPOD" of each activity should be measured separately by identifying:
1) the maximum recovery time period
2) the minimum acceptable level of each activity within business continuity period, after consulting with top management;
3) the maximum period whereby normal activities can be proceeded with until return to normal activity.
e) During BIA, main/essential activities whereby the entity's main services and functions are delivered should be identified. Hence, such functions should be recorded.
f) Classify and prioritize such activities for recovery established by the BIA;
g) Recording all suppliers and contracting parties which perform specific roles during entity's BC operations.
h) Approved plans may be available at some Entities and hence they will not be required to start from scratch. Accordingly, such plans along with the previous BIA mechanism shall be reviewed and adopted whenever deemed valid.
i) Predetermined plans for suppliers and outsource partners may be in place. Such plans shall be reviewed, to ensure their conformity with the Standard and whether they meet its requirements.
j) All external sources of required resources for BC should be identified and arranged in lists with the suppliers of these requirements or material.
k) According to a risk technique study, there are some acceptable risks and proper scenarios were established to handle them. Thus there is a specific time set for recovery and continuity in delivering activities.

A.8.5 Risk Assessment

While BIA helps identify some of the BC risks, a comprehensive threat and vulnerability assessment is still required to identify a wide range of risks and the probability of their occurrence.

To collect this information, further interviews are conducted with individuals in support fields such as IT, General Services, and Security to identify single points of failure (SPoF) and threats that could cause them to fail.
These interviews can be based on information from previous assessments that is gathered, reviewed and updated to review such assessment, or on those obtained in a new assessment.

There are many Risk Management models, some of which are general; others are developed for use in specific industries or sectors.
These models have certain elements in common, including the identification of specific threats (or hazards, the use of a mathematical formula to calculate risk value. Such formula involves a combination of numeric ratings for impact, likelihood, and vulnerability.
The rating for impact represents the size or scale of potential loss / damage resulting from the event
The rating for likelihood represents the probability of an event's occurrence
The rating for vulnerability reflects the reduction in expected loss provided by controls and preventive measures the entity has put in place to reduce severity of impact

Each entity should apply a common framework for Risk Management and Risk Assessment across its business locations, operations and departments. It should not create one framework for Risk Management and another for Business Continuity.

Threats to continuity of the entity's main / essential activities include by way of example but not limitation:

- Floods or water damage
- Natural disasters
- Unavailability of key persons
- Fire
- Power failure
- Air conditioning failure
- Data transfer and Voice Communications failure
- Technical failure
- Theft
- Willful damage by insiders
- Willful damage by outsiders

Should an incident occur due to one or more of these threats, it may impact the entity in terms of health and safety of personnel responding to the event as well as those affected by such event

- Performance of main/essential functions and activities during and following such event
- Use of main / essential property, facilities, assets and infrastructure
- Ability of internal and external transportation systems in its supply chain to deliver products and services

- Reputation or confidence in the entity's ability to perform its duties, functions and services
- Short and long-term financial losses
- Environment

A Risk Assessment can be performed by completing the following steps:
List the recognized internal and external threats that could result in disruption to entity's main/ essential activities, as identified by the BIA.
Develop a system to be used for impact, likelihood and vulnerability measurement.

Review the list of threats and the recommended measurement system with Top Management, and obtain their approval.
Determine the likelihood for each threat and assign a value based on the scoring system.

Determine the entity's vulnerability to each threat and assign a percentage value that represents the expected impact reduction that the controls and mitigation measures are expected to produce.

Calculate the risks of each threat by combining the scores for impact, likelihood and vulnerability.

The most common method to calculate risk is as follows:
Risk = Likelihood x Impact x Vulnerability
Prioritize the threats by overall rating of the level of risk.
Identify unacceptable risks.

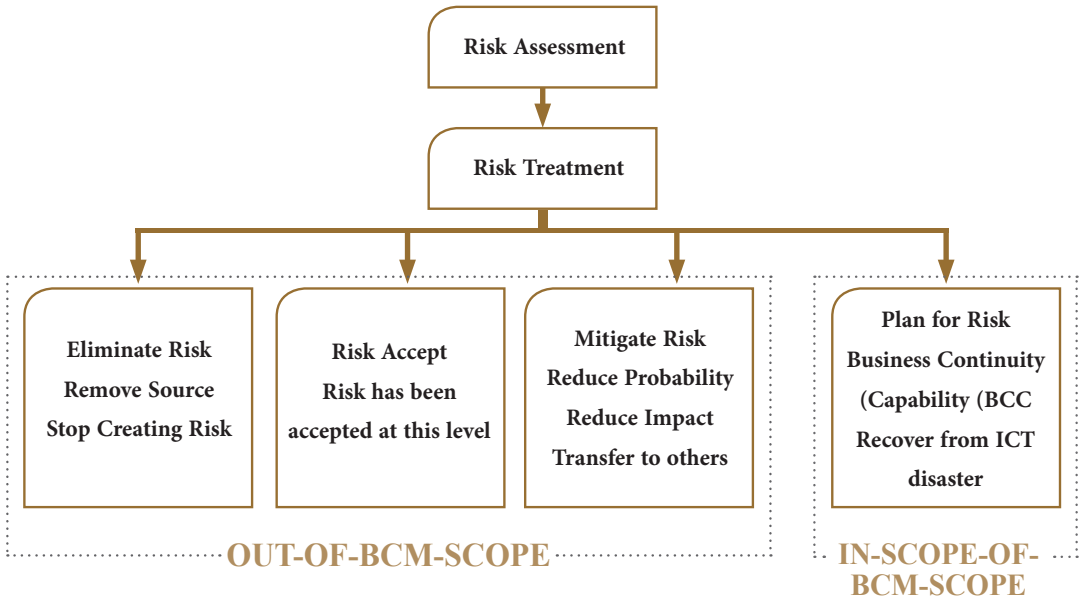
Provide a copy of the risk assessment results to the entity's Risk Management program officer.

Identify the actions required to reduce the disruption threat to main / essential activities in a report submitted to Top Management.

Risk Assessment outcomes should include the following:
- Threats could result in the disruption or suspension of the entity's main/ essential activities, classified by level of impact
- Single points of failure (SPoF) associated with such threats
- Actions required to reduce the threat of disruption or suspension of the entity's main / essential activities

All risks identified in the Risk Assessment should be recognized in a Risk Register, or Risk Log, along with information on the mitigations, preventive and corrective actions required in order to reduce such risks.
The risk log is a 'living document' that is updated at least annually or whenever a major change occurs in the entity's business process, locations and facilities, or operations related to its main / essential activities.

A part of the Risk Register identifies the risk treatment techniques to be applied to the risks identified in the Risk Assessment. There are essentially four categories of risk treatment techniques as shown in the figure below:



Risk Acceptance – used when Risk is at a level below the entity's risk appetite, or the cost of dealing with the risk outweighs the benefit.

Risk Mitigation – used when Risk can be reduced to a level below the entity's risk appetite.

Risk Elimination – used when Threat or Vulnerability can be removed.

Risk Planning – used when the above treatments are applied but the entity still endures an unacceptable level of risk. Therefore, a BC Plan is developed to identify the required response actions and procedures and regain BC capability in the event of business disruption.
Each risk treatment process should be implemented by the person in charge of it.

Where treatment lies in "BC planning", a BC plan shall be developed by the departments/staff responsible for performing main / essential activities. Such plan shall identify the work areas, personnel, tools, equipment, systems, data, and information required to ensure the continuity of these activities within timeframes established by the BIA.

The Risk Register should be maintained by the Risk Manager and subject to Audit at least once a year. For instance, there are several ways Entities can handle business disruption risk:

If the risk is caused by concentration of main activities in a single location, the entity can arrange to have such activities performed in two locations, as long as they are not susceptible to disruption by same event.
If the risk is tied to the use of out-of-date facilities, equipment, or procedures, it can replace or upgrade them.
Where providing multiple locations, replacing or upgrading the facilities, equipment or procedures can be too costly; an entity can buy insurance to reduce loss value.
Another option is to rent the facilities and/or equipment, or to contract performance of the work out to another entity which may not be subjected to the same risk.

A.8.6 Risk Treatment Strategy
Once a Risk has been identified, a Risk Treatment strategy should be developed and recorded in the Risk Register. Risk Register should include:
- Risk-related tasks;
- Responsibilities entrusted to specific individuals or positions, to ensure tasks performance;
- The date when such task shall be completed;
- Resources required to complete the task; and
- Name of the person who approves task completion.

A cost-benefit analysis can be used to select the most appropriate risk treatment strategy. Other techniques that may be useful include:
- SWOT Analysis (Strengths / Weaknesses / Opportunities / Threats);
- PEST Analysis (Political / Environment (or Economic) / Social / Technical impact); and
- Market analysis to determine the product viability following a major disruption in the supply chain.

In many cases, a number of treatments can be applied to a risk and the overall

strategy may require a combination of treatments to reduce the risk to an acceptable level.

Where BC Planning is recognized as a risk treatment option, the following shall be taken into account:

Back-up Sites (Split/ Dual site operations)
This strategy involves performance of main / essential activities at two or more geographically dispersed sites so operations continue from other site when one site fails. These arrangements are two ways i.e. any site fails, the other continues to deliver. Both sites are in full operation technically during BAU (business as usual) times. This is suitable, especially for financial or security entities, where the recovery time objective "RTO" is measured in minutes or hours rather than days.

Alternative Sites
A strategy similar to the back-up sites strategy involves the use of another facility to perform the entity's main/essential activities at a site geographically dispersed from the primary site. Using this strategy, the first site can be operational and in use while the other is inactive but available for use. An actively ready site is commonly known as a 'hot' site and an inactive site which is ready for use is commonly known as a 'warm site'. Where arrangements to build or renovate a site in times of emergency, crisis or disaster rather than at a previous time are conducted, such site would be known as 'cold' site.

Implementing this strategy involves moving personnel to the back-up site after an emergency, crisis or disaster strikes. The alternative site may be a facility provided by a third-party, an entity's facility or a common site which is related to the local or federal government. A 'hot site' strategy is good where RTOs are very short (in minutes); a 'warm site' strategy is good for relatively longer RTOs (in days); while a 'cold site' strategy works well when RTOs are very long (in weeks and months). Staff can be moved to the alternative site quickly enough, to continue performance of main / essential activities within RTO. The success of this strategy depends on whether staffs are able and willing to work at the alternative site for a prolonged period of time where necessary.

Outsourcing
Another strategy that can be employed to reduce risk is to outsource or contract performance of critical activities to a third-party depending of course on the nature of entity's business and services. To that end, MOUs shall be

concluded with outsourcers. This option may be preferable in manufacturing, where the added cost incurred to establish back-up or alternative sites might be higher than the benefits resulting from the project.

At times, the only outsourcing option might be to enter into contract with another entity that is engaged in the same type of business, which could be a competitor. In this case, the benefits of risk treatment need to be weighed against the risk of creating dependency on a competitor. Such arrangements are also known as 'mutual aid arrangements'.

As regards short- RTO products and services, outsource contracts shall be concluded in advance. However, when it comes to products and services with longer RTOs, it may be possible to wait until after the event to conclude the contract. There is, however, a risk in waiting until after an event has occurred to establish a contract – for, by that time the outsource partner may be fully committed and unable to meet the entity's needs.

Outsourcing or contracting the performance of main activities to third parties does transfer the risk, but does not discharge the entity from its legal liability to provide the products and services to its stakeholders.

Post-Event Procurement

An additional strategy that can be used for products and services that have their RTO measured in days or weeks is to purchase such products and services from vendors and suppliers that can provide the same on short notice whether for the public or private sectors.

This strategy poses the same risk as waiting until after an event to establish outsourcing agreements, the vendors and suppliers may have used their available stocks to meet the needs of other clients. To prevent such a case from arising, the entity may consider warehousing a temporary supply of essential materials for continuity of its main / essential activities.

Post-Event Procurement strategy is not suitable for products or services that require special equipment or facilities, or skills that are not readily available, or that require more time to master such as medical services or customer services at various departments.

Insurance

Insurance can be purchased to provide financial compensation for loss of assets, cost of recovery and protection of legal responsibilities.

However, insurance is unlikely to cover all costs resulting from a disruption,

including the loss of customers, shareholder value, reputation, life or trademark image.
Contingent Business Interruption insurance can, in some cases, be purchased to cover direct costs related to loss of revenue as a result of disruption of main/essential activities. However, this type of insurance only covers business losses which are tied to another insurable loss (e.g. damage to a building, work area, or tools and equipment used in such areas, including IT and non-IT systems). Another type of insurance that is beginning to appear on the market involves coverage of a wider range of interruptions and disruptions including failure in the supply chain. Other types of insurance that may be necessary to protect against risk include Kidnap and Ransom or Errors and Omissions (professional liability).

Manual Workaround
Most business environments today are automated and dependent on the systems, tools, and equipment that either automate or support its critical activities. In some cases, risk treatment can be as simple as using a manual process, alternative technology and tools, or paper-based documentation following a disruption.
Such paper based work carried out during recovery needs to be reflected back on to systems when the systems are available. Hence, the systems should be designed with a capability of accepting such transactions.

Cross-training
A very common risk occurs when there is only one person who can perform a critical activity, such as signing cheques, contracts and work authorizations, maintaining a particular system or piece of equipment, or leading development of a new product or service. This risk can be treated by cross-training others to eliminate the single point of failure and ensure continuity of operations. Some staff can be trained on professional jobs to perform such important jobs identified in the BIA.

Resilient IT Architecture
IT systems in particular have many single points of failure. Risk due to single points of failure can be mitigated by analyzing the system to locate them in the entity's hardware, software or networks.

Once a single point of failure and the system vulnerabilities that create it are identified, options can be developed to reduce the risk by providing failover or rerouting.

IT resiliency solutions include high availability architectures such as cloud computing, neural networks, failover software solutions and disk arrays. There are special standards for BCM technical solutions in IT field.

Occupational Health and Safety and Environment (OHSE)
The risk of damage to the entity by injury, loss of life, or destruction of property can be reduced by the use of HSE procedures. Such procedures help reduce the risk of fire, flood, hazards, contamination, and the spread of infectious disease in the workplace.

Third-Party Review
Much of the risk arising from the use of Third Parties and suppliers can be addressed by due diligence in the procurement and contract process. This includes:

- Code of conduct / business ethics
- Corporate social responsibility
- Attention to environment
- Health and safety
- Import and export
- International standards, including Business Continuity
- Quality Management
- Regulatory and contractual compliance
- Risk management
- Security level

The remainder can be addressed by a review of the third-party / supplier BC capability programs. A good approach is to ensure that many of these risks are assessed and treated in the procurement and contract process, then measured and reassessed through the entity's business.

A.8.7 Business Continuity Strategies
Identifying the entity's risk treatment strategy will determine which products and services require a Business Continuity strategy to ensure the continuity of its main/ essential activities.
BC strategies should be coordinated or integrated with other plans, strategies and budgets the entity has in place, so as to ensure there is no conflict of interest.

To ensure success, the BC strategies shall determine:

- The party which is responsible for achieving the recovery goals

- Means and resources to be used to achieve the goals
- The timeframe set for achieving the goals
- Determining the best strategies which ensure many factors are taken into consideration. Of these:
  1. Results of the entity's BIA and risk assessment
  2. Costs of implementing the strategy or strategies, and
  3. Consequences of disruption.

Strategy is based on prevention, redundancy and recovery. In defining its BC Strategy, the entity shall take into consideration all elements required to ensure the continuity of its main / essential activities. This includes:

- Main / essential Assets;
- Information;
- Premises;
- Staff;
- Stakeholders;
- Supplies;
- Supporting infrastructure; and
- Technology.

The entity's BC strategy may be accomplished by developing one or more BC Plans. In doing so, each plan may address specific aspects or components of the entity's operations, or all operations at a single location. Whether the entity opts for a single BC plan or multiple plans, the key responsibilities, resources, programs, and activity outcome need to be adequately and fully defined in each plan.

A.8.8 Business Continuity Plan

The effectiveness of an entity's Business Continuity capability is dependent on its ability to plan for activity at each stage of the disruption.

First, the entity shall effectively respond to the incident to ensure the health and safety of its personnel, those responding to the incident and those impacted by the emergency, crisis or disaster. In many cases, the information required for this purpose is contained in the entity's Building Emergency Plan or in a separate plan known as the entity's Incident Management Plan.

Second, the entity shall coordinate the activities of those responding to the incident; perform the initial damage assessment; organize the Incident

Management team responsible for identifying the required actions, coordinating the activities of response teams and approving the communication to internal and external stakeholders. This information is included in the Incident Management Plan. As part of the incident management process, an entity shall deliver messages to internal and external stakeholders to keep them informed of the status of the entity's response and recovery activities. This information is usually contained in the Incident Management Plan or a separate plan known as the Crisis Communications Plan.
External means of communication include:

- News or press releases
- Media
- Financial reports
- Newsletters
- Websites
- Phone calls, emails and text messages (manually delivered and/or via automated emergency notification systems)

Finally, once the entity is able to regain the continuity of its main/essential activities, it shall develop a plan that identifies the teams, processes and procedures that will be used to perform such works. This information is contained in the BC Plan.

The Incident Management Plan of Top Management, Executives and Senior Managers provides the instruction and guidance needed to coordinate the activities of teams involved in responding to, stabilizing, and recovering from, business disruption incidents. The Incident Management Plan should provide response to an incident by:

1. Defining the criteria of response plan activation;
2. Identifying who has authority to activate the plan;
3. Activating or forming the Incident Management Team;
4. Identifying the key areas to be considered and recording the same in brief guidance bullets to ensure they are addressed;
5. Activating or establishing alternative sites for:
   - The restoration of IT or other main/essential infrastructure elements
   - Temporary use of any element in performing main/essential activities
6. Recording the internal and external stakeholders to be contacted in the first few hours of an emergency, crisis and disaster;
7. Defining the means of communication with stakeholders, local authorities, and media and what is required to be communicated to them;
8. Providing pre-scripted message templates for communications;

9. Identifying the personnel responsible for coordinating with first responders; and
10. Identifying process and criterion used to assess damage and impact.

The Incident Management Team should be comprised of two groups. One is the Core Group, and consists of representatives in key business areas that would meet in any type of incident. The other is a Support Group, which consists of representatives from business areas that would be contacted depending on the nature of disruption and its impact.
There is no specific list of business areas to be represented in each team; however, representatives of the business areas listed below are often found in each of the teams.

Core Team:
- Incident Management Leader (appointed by Top Management);
- Information Technology representative;
- Support Service or Facilities representative (liaising with Damage Assessment team);
- Communications / Media Relations representative;
- Business Continuity Manager; and
- Scribe (to log minutes of meetings and decisions).
- Support Team
- Human Resources representative;
- HSE representative;
- Security representative;
- Legal representative; and
- Operation and Business Support representatives.

To ensure each team is able to perform its function, the entity should appoint one person as Primary and another person as back up for each position in both Core and Support Teams. The Incident Management Plan should be concisely developed. It should identify the tasks to be performed and provide the basic information required to perform such tasks. Checklists and bullet points are commonly used in this type of plan.

(See 'BC Toolkit 1 – Templates' for an Incident Management Plan Template and 'BC Toolkit 2 – Examples' for a sample plan).

The entity's Communications Plan should provide instruction and guidance required to Top Management, Executives, Staff and Public Relations personnel on how to communicate approved messages with internal and external stakeholders before, during and after business disruption.

This plan should include a predefined structure of the process of gathering and publishing information on the emergencies, crises and disasters to internal and external stakeholders.

Also, the plan shall identify key partners and persons who will be responsible for communicating with each partner group, before, during, and after an event. Pre-scripted message formats should be included as part of the Communications Plan.

Various methods can be used for delivering messages to key partner groups. These include:

- Automated notification systems;
- Emergency call-in numbers ('hotlines' by virtue of recorded messages providing current status and updated information on the event);
- Call centers;
- Publication via email or voicemail;
- Status or update postings to the entity's internal website; and
- SMS.

Entities should evaluate the need for alternative methods and/or additional systems and be prepared for system overload or failure during an emergency.

(See 'BC Toolkit 1 –Templates' for a Communications Plan Template and 'BC Toolkit 2 – Examples' for a sample plan).

A.8.8.1 Prior to developing its Business Continuity Plans, the entity shall develop or review and update existing documentation that define the recovery objectives its plans need to achieve, e.g. Risk Assessment and Business Impact Analysis. The assumptions used in developing such plans should also be identified and reviewed at the beginning of the planning process. These assumptions should be consistent with the results of the entity's risk assessment, and impact analysis. Confidential or sensitive information needed to implement the plan can be stored in a separate document, with appropriate levels of security and protection, to ensure the document and its contents remain confidential.
In the case of a small-sized company, BC plan may consist of a single document. However, where the entity is large-sized or complex, BC information may be contained in a series of documents and often a separate plan is developed for each department or section of such entity.

Where BC plan is contained in a series of documents, the entity should ensure plans are well- coordinated and organized to provide the information required for response, incident management, communication with stakeholders and continuity of main / essential activities.

Below are some examples of how to develop BC plans for variously-sized Entities:

Small-Sized Entities: Single Plan, Single Site
In a small, single-site entity, all levels of response are recorded in a single plan with a single incident management team responsible for carrying out the entity's activities and works.

Medium-Large Sized Entities: Multiple Plans
In a medium sized entity, the levels of response are recorded in a number of plans, which are implemented by more than one team.

Incident Management Plan consists of a team composed as described in Section 8.8 above;
Business Continuity Plan for recovery of all the organization's operations, with a response team of operational management personnel;
IT plan, which details the procedures and techniques of technology recovery;
Human Resources Plan to deal with accounting for staff, managing the recording of injuries and fatalities, trauma counseling and general personnel issues;
Facilities Management Plan to assess site damage, provide security services at both main and alternative sites, prepare alternative sites, and communicate with Emergency systems, etc.;
Damage Assessment Plan for the Facilities and IT teams to be used to assess emergency, crisis or disaster impact; and
Other plans specific to scenarios relevant to business functions, i.e. plane crash plan for airports and oil spill plan for the maritime and oil entities, etc.

Multi-National Entities: Multiple Plans, Multiple Sites, Multiple Regions
In large multi-national entities, the levels of response are recorded in a number of plans, which are implemented by more than one team:
A global Incident Management Plan, with a response team composed of members with global responsibilities and one or more regional Incident Management Plans with response teams composed of Senior Managers with regional responsibility.

Operating pursuant to the instructions of the regional incident management team, a set of Business Continuity Plans for each field which covers a major division, product, or service area – each with its own response team of operational managers responsible for areas covered by the plan.
Other plans as described in the Medium-Large Entities plans.

A.8.8.2 In addition to all items stated from A to N in the Specifications section of this document, an entity should develop its Business Continuity plans by following procedures and operations, which include the following steps:

(a) Appoint someone to be responsible for development, update and maintenance of the plan;
(b) Define the plan's objectives and scope;
(c) Develop and approve the plan development process;
(d) Create the team(s) that will implement the plan;
(e) Assign responsibilities for response, incident management, communication, and re-establish continuity of operations;
(f) Decide the structure, form, elements and components of the plan(s);
(g) Determine the strategies governing the plans, e.g. The use of an alternative work site;
(h) Gather information to populate the plan;
(i) Integrate the plan with third-party plans and procedures;
(j) Draft the plan;
(k) Circulate the draft for review and comment;
(l) Duly revise the draft;
(m) Validate the plan's final content, for example by conducting a plan walk-through or tabletop exercise; and
(n) Identify the training and maintenance activities and develop a schedule to perform them and to use the results of such trainings to maintain the validity and effectiveness of the plan(s).

The stakeholders in an entity's Business Continuity capability include people with special needs. These special needs shall be taken into account when planning.

Special needs populations include people with physical, mental health, development and learning, visual, auditory, or non-visible disabilities; people with mobility difficulties; people who live in institutionalized settings; elderly or very young individuals who are dependent on others for their primary care; pregnant female workers and those who have limited proficiency in the local language.

A.8.8.3 Contents of BCM Plans

In addition to the points set out in the specifications, we would like to emphasize some important points and issues. All BCM plans should include those held responsible for ensuring the health and safety of the entity's employees, contractors, visitors and customers. Regardless of BCM plan contents, where such plan is implemented onsite, directions and instructions issued by emergency services personnel prevail over instructions and directions given by the entity's own staff, even if contents of the BCM plan are integrated.

Another important item required by each to be used in building-related emergencies and evacuation is an 'Emergency Box', or 'Go Bag'. The 'Emergency Box' contains required equipment and supplies for major incidents. It contains the items immediately needed for safety and security purposes.
(See 'BC Toolkit 2 – Examples' for an example of the contents of the Emergency Box).

If the 'Go Bag' has battery operated equipment, then the validity/charging of batteries should be ensured through periodic checks.
BCM plans provide for site security and personnel, and the activities needed to regain continuity of its main/ essential activities once emergency services personnel have handed control of the site back over to the entity.

BCM plans shall include the processes and activities to be carried out, from incident response to continuity regaining and return to normal operations. As regards departments managing infrastructure, BC plans shall identify the processes and activities to be carried out to restore existing services or alternative facilities to support the recovery of other business units.

The Incident Management Plan provides guidelines on how strategic issues resulting from a major incident will be addressed and managed by the entity's Top Management. The Incident Management Plan should determine team activation method so that action can be taken to respond as quickly as possible after a disruption occurs. At least two locations should be identified in the plan to be used as an incident management command center (or 'control room'). The main site is usually the operational site where operations and functions are carried out. The alternative site should be located at a reasonable distance from the main site, so it is not likely to be impacted by the same event.

Operational plans should identify a list of resources required to activate the plan. This may include:

- Employee
- Security
- Transportation logistics
- Social needs
- Emergency expenses
- Facilities
- Incident Command Center
- Recovery sites
- Infrastructure
- IT BC Plan includes:
- Applications
- Technology Services Methods to manage and control documentation and records
- Communications
- Information (which may include)
- Policies;
- Standard operating procedures;
- Work instructions;
- Internal and external contact details;
- Financial (e.g. payroll) statements;
- Staff names, contact details and next of kin;
- Customer account records;
- Supplier and stakeholder details;
- Legal documents (e.g. contracts, insurance policies, title deeds, etc.); and
- Other service documents (e.g. contracts and service level agreements).
- Supplies

The entity should draft in advance the message templates, scripts, and statements it may need to communicate with stakeholder groups regarding threats identified in the risk assessment. It should also include the procedure of delivery of these messages on short notice so messages can be promptly delivered depending on the extent of incident significance.

The entity should designate key and substitute official spokespersons especially those trained on media talking and communicating with internal and external stakeholders.

A.8.9 Awareness and Training

Awareness and training ensure the entity's personnel and staffs are aware of the importance of business continuity, understand their roles in implementing its plans, and have the knowledge and ability to implement its plans.

Training can be provided through internal or external sessions and working with professionals assisting in BC program development and implementation. To ensure BC tasks are given appropriate time and effort, the roles and responsibilities for performing them should be integrated into job descriptions and the job performance appraisal process.

The awareness and training strategy varies from one entity to another, depending on each entity's strategy and policy.

A.8.9.1 Staff Awareness
The entity's level of awareness differs as personnel join and leave the organization. Internal and external events may also lead to a spike in awareness and sensitivity to business continuity issues.
Items which should be addressed in general staff awareness of the entity's BC capability include:

- Identification and escalation of incidents
- Triggers for incident response and activation of business continuity plan(s)
- How to respond to special events
- Measures to be taken during site evacuation are in place for response, incident management, business continuity and recovery plans to be available

Items that shall be available to boost awareness among specific teams in the entity's BCM program include:

A (a) a measurable and assessable system should always be developed to ensure the effectiveness of the awareness program by obtaining periodic data or holding interviews with staff to determine the extent of their understanding and awareness with respect to the BC program.

A (b) This awareness can be spread within the entity through the Risk Management Section or BC Manager by holding continuous awareness courses as well as placing purposeful posts in staff gathering areas to

remind them of the importance of being prepared for emergency. This should be an integral part of the entity's work environment culture.

A (c) Continuous Improvement of the program should be conducted by attending specialized scientific conferences and seminars whether tailored to the entity's emergency staff or Top Management to support their understanding of the importance of these programs.

A (d) Staff playing roles in the BC program should be encouraged through financial and moral incentives because in many cases these tasks are an addition to their original tasks. So, their efforts should be properly appreciated, especially after holding annual exercises or real incidents.

BC awareness scope expansion should be considered with respect to the entity's suppliers, customers, contractors and external stakeholders.

A.8.9.2 Training
A.8.9.3 Training Logs
All personnel should receive proper training to be able to perform their BC-related duties. They should also receive instructions on the key components of the entity's BCM program, in addition to the response and recovery plans that directly affect them.

The entity's training should include procedures for evacuation, shelter-in-place, check-in at the evacuation site, responsibility towards employees, activation and preparation of alternative worksites, and handling of requests for information by internal and external stakeholders.

Response and recovery teams should receive education and training on their responsibilities and duties, including how to interact with first responders. Teams should be provided with initial / refresher training at regular intervals and a suitable mechanism should be put in place to ensure new members are trained when they join the team.

Core topics in meeting the training needs among specific teams in the entity's BC capability program include:
- Overview of Business Continuity Management
- Program Management
- Business Impact Analysis (BIA)
- Risk management

- Strategy Development
- Incident Preparedness and Response
- Development and implementation of Business Continuity plans
- Development of Awareness and Training Program
- Exercising, Updating and Maintaining BC plans

Other subject areas may include:
- Damage assessment
- Restoration of facilities and equipment
- Public Relations and Crisis Communications
- Business Continuity Management Audit
- Developing IT Recovery and Continuity Strategies
- Emergency and Crisis Management
- Team Leadership
- Testing the tools and equipment required to implement BCM plans

(See 'BC Toolkit 4 – Training' for a list of accredited training providers and associated courses).

A.8.10 Test and Exercises

A.8.10.1 Tests

A.8.10.2 Exercises
Tests and exercises are activities designed to assess the ability of the entity's personnel to respond, manage, communicate with stakeholders, continue to perform assigned duties and recover from various scenarios of business disruption.

Exercises and their outcomes constitute the foundation whereby BC capability would be determined.

The entity should design test scenarios that focus primarily on training on highest risk business activities, as identified in its risk assessment and impact analysis. Also, the entity should conduct exercises and record the results of such exercises to ensure BC plans, processes and teams are effectively achieving the recovery objectives of the entity. Exercising ensures teams and personnel are adequately trained to use and operate the tools, equipment and other resources needed to perform their duties. An exercise is commonly done by simulating the entity's response to an incident, rather than fully

activating the teams, plans, and resources that would be used in a real event. These simulations can be announced or unannounced. The purpose of the exercise program is to enhance the overall performance of the entity's BC capability.

Exercises should be developed and conducted to:

1. Apparent weaknesses and strengths in the plans, operating procedures, and planning assumptions;
2. Ensure the entity's BC Strategies are accurate and its BC plans will enable the entity to meet the recovery objectives defined in its BIA;
3. Ensure cohesion and integration of plans in terms of interoperability;
4. Test and validate recently changed procedures;
5. Familiarize BC and Incident Management Teams with their processes and procedures;
6. Ensure personnel and teams implementing the plans and procedures have the requisite skills, authority and experience to implement such plans.
7. Enhance coordination among response agencies and support organizations;
8. Validate the training process and procedures for evacuation, response, incident management, communication, and regaining of business continuity; and
9. Increase the entity's awareness and understanding of the threats which can impact and disrupt its critical activities.
10. Validate that all the contacts and information necessary to attain recovery resources required by the plan, have been accounted for.

The entity's BC Exercise Program should ensure that all personnel and elements of BC plans are exercised over a period of time in such a way as to avoid disruption to normal operations.

A process that can be used to develop an effective test and exercise program involves the following steps:

- Cooperate with Top Management to identify the entity's BC capability areas that would benefit from the increased awareness that an exercise would provide.
- Identify the BC plan elements, resources and procedures that will be exercised, e.g. resource allocation, emergency contact and communication, or relocation to an alternative worksite.
- Identify a suitable exercise for each element, resource or procedure.
- Identify the personnel or groups involved in the exercise.
- If exercises have been conducted in the past, review the supporting documentation to avoid using the same scenario or personnel and to identify the activities that require further exercising / testing.
- Create a timetable to ensure that, over time, the scenarios are capitalized

on, which would have the greatest impact on continuity of the entity's critical activities.

The frequency of tests and exercises are dependent upon the nature, size and complexity of the organization.

Each member of the entity's Incident Management Team, including representatives, should participate in an exercise at least every 12 months.
Other events which may initiate the requirement for an exercise include significant changes in the entity's:

- Location or facilities
- Operating environment
- Tools and technology
- Key personnel
- Suppliers and service providers
- Outsource partners
- Use or purchase of critical assets
- Business objectives
- Rules & Regulations
- Standards

A Test and Exercise Plan should be documented before each test, highlighting the:

- Objectives:
- Success criteria;
- Timetable and schedule of activities;
- Resources used;
- Risks;
- Assumptions;
- Exclusions.
-

(See 'BC Toolkit 1 – Templates' for a Test and Exercise Plan template).

A Test and Exercise Report should be completed immediately after the completion of each Exercise. This report should, at a minimum, contain:

- Management Summary
- Introduction
- Background
- Results summary
- Summary of exclusions and issues
- Corrective and Preventive Action Plan
- Independent observer report

(See 'BC Toolkit 1 – Templates' for a Test and Exercise Report template).

A list of exercise types and processes that can be used to help select and design exercises figures in the table below.

Type of test	Process	Participations	Frequency	Complexity
Desk Check	Check the structure and elements of the plan	Author of plan	High	Low
Walk Through	Discuss the theory of the plan to check that it is usable	Author of plan Users of the plan		
Simulation Or Discussion Exercise	Use the plan to undertake theoretical response to an incident	Coordinator / Emergency Officer Users of the plan Other as required (e.g. observers)		
Unit Test	Confirm that a recovery procedure or the recovery of a piece of technology works	Users of the procedure of technology Other as required (e.g. Technicians)		
Unit Rehearsal	Practice a recovery procedure or the recovery of a piece of technology, following a script	Procedure or technology users Other as required (e.g. Technicians) .		
End-to-End Test	Confirm that the recovery of a complete are of the organization (a business process, product or service, or inter-connected technologies) works	Those in the area of the organization or those that are required for the business process, product or service or users of the interconnected technologies. Other as required (e.g. Technicians)		
Full Rehearsal	Practice the recovery of a complete area of the organization, a business process or services or inter connected technologies, following a script	All those in the area of the organization or those that are required for the business process, product or service or users of the interconnected technologies. Other as required (e.g. Technicians)	Low	High

Methods and Approaches

To be successful, an exercise program shall begin simply and escalate gradually.

A.8.11 BCM Continual Improvement

A.8.11.1 Requirements
On a regular basis, at least annually, the entity is required to perform a review of its BIA, Risk Assessment, BC Strategy, and Plans. This review is designed to ensure all BC capability documents are valid and consistent with the entity's strategic objectives.
This review should be formally conducted by the Internal Auditor or Business Continuity Manager. The review should result in a report to Top Management. Review and update are necessary when a change occurs in the entity whether in terms of services or works or when a change occurs within Top Management.

A.8.11.2 Methodology for Continual Improvement of the BC Capability
The following procedure can be used for periodic review and continual improvement of the entity's BC capability.

Scope and Objectives
The reviewing person / team should initially advise the entity's management that the review is about to take place, to ensure the correct persons are available to conduct the review. The review should be scheduled as a formal meeting with the functional or departmental Business Continuity participants. Documentation of the meeting should include all action plans and agreements required to implement such plans. Any newly identified risks should be added to the Risk Register. The first meeting should be held with Top Management to determine whether substantial changes to the entity's objectives and direction have or have not already been addressed. Any changes not yet identified or addressed should be assessed for impact on the entity's BC capability. Updates to the BC program scope should be made where and when necessary.

Business Impact Analysis Review
Meetings held with functional or departmental Business Continuity co-coordinators should involve discussion and review of scope-related changes. They should also involve updates to the BIA which result from such scope changes.

Risk Assessment Review
The Risk Register should be updated if need be, in consistency with changes in the entity's BC Strategy. Action that has been taken, or needs to be taken,

to treat risk in accordance with changes in the entity's BC Strategy should be recorded in the Risk Register.

Strategy Review
The updated BIA should be assessed against the entity's response, continuity and recovery capability. Any gaps in updates to the entity's BC Strategy should be addressed.

Plan Review
Plans and procedures should be reviewed to ensure updates are made in accordance with changes to the entity's BC Strategy as well as the infrastructure required to implement such Strategy.

Plan reviews should also take place between the entity and its critical third parties (e.g. suppliers, vendors, and service providers). The entity's plans as well as those of its third parties will effectively help meet its recovery objectives.

Test and Exercise Review
An entity's BC plans and procedures should remain fit for purpose. The primary method to ensure this is to conduct tests and exercises using scenarios that demonstrate whether the entity's BC plans and procedures are effective in meeting its recovery objectives.

The reports emanating from these exercises should be reviewed to ensure the entity has suitably demonstrated that its Plans are fit for purpose. Major changes to plans and procedures should be tested and exercised at the earliest opportunity to validate the entity is maintaining its BC capability.

A.8.11.3 Results (BC Capability Report)
The BC officer should review entity's Business Continuity Program so that a BCM capability report is issued. This program contains the information which ascertains that the entity's BC capability is still fit for purpose. The report should demonstrate the entity's capability to support its strategic and operational objectives. The report should be supported by information from the entity's BC capability test and exercise program. The report should also address any non-conformities and risks requiring treatment that either carry over from or have been identified since the previous report.
(See 'BC Toolkit 1 – Templates' for a BC Capability Report Template and 'BC Toolkit 2 – Examples' for a sample report).

A.8.11.4 Non-Conformities
An investigation should be conducted to identify nonconformities, to develop a corrective action plan to address the problems, mitigate consequences of nonconformity, and apply required changes to remove the cause of nonconformity with the Standard.

The nature and timing of corrective action should be appropriate to the size and nature of nonconformity and its potential consequences. Top management should ensure corrective and preventive actions have been implemented and that there is systematic follow-up to evaluate their effectiveness.

A.8.11.5 Preventive and Corrective Actions
It is essential that the entity operates within the limits of its Risk Appetite. Any situation which puts the entity at risk of exceeding its Risk Appetite should be subject to Preventive and Corrective Action. This action should be recorded in the BC Capability Report or an Ad-hoc Non-Conformity Report. Preventive and corrective actions should be compared to BCM objectives and policy to ensure continual conformity.
(See 'BC Toolkit 1 – Templates' for an Ad-Hoc Non-Conformity Report Template and 'BC Toolkit 2 – Examples' for a sample report).

The non-conformities and treatment options chosen for them should be followed up to ensure that appropriate action is taken, priority is assigned to that action, and authority given to those responsible for that action to provide successful risk treatment. Corrective and preventive actions that result in changes to the plans, process and procedures of the entity's Business Continuity capability may also trigger a review of the risk assessment and impact analysis related to the changes.

A.8.11.5.1 Preventive Actions
The Preventative Action process should involve identification of risks and potential risks. In most cases, this can be accomplished through entity's Risk Management, by following established procedures.
Where an established Risk Management function or procedure does not exist, the entity should identify, and record risk treatment, in accordance with the Risk Assessment methodology used in implementing its BC program. Where a Risk Assessment methodology does not exist, the entity may consider adopting the methodology used in its quality improvement program.

A.8.11.5.2 Corrective Actions
The corrective action process should be initiated as part of the investigation after each incident or exercise.
It can also be initiated (plan improvement) during the incident if such incident is going to extend over a long period of time.
The process should include:
Development of a statement that describes the problem and identifies its impact and reasons;
Review of corrective action from previous evaluations and identification of solutions provided;
Selection of a strategy, prioritization of action(s) to be taken according to their importance based on specific schedule;
Identification of the resources required to implement the strategy;
Provision of authority and resources required to accomplish the changes;
Monitoring progress of corrective action through completion;
Verification that the problem is resolved through exercise or test of the solution once the corrective action is complete.

A (a) After BIA and risk assessment have been conducted, the gaps found should be promptly remedied in order to control entity's BC if an emergency occurs, consequently these gaps are given priority for treatment.

A (b) the significance and size of such preventive action should match the size of expected impact when an emergency occurs, which would determine the size of the budget, where required.

A (c) the requirements needed to clarify preventive action documentation are as follows:

- Identification of potential non-conformities and reasons
- Identification and implementation of the required preventive actions;
- Recording and review of the results of taken actions in the preventive actions log;
- The entity's BC Manager should retain a list of taken actions, especially if any non-conformity exists.

A.8.11.6 Conformity and Certification
Conformity and Certification should constitute an ongoing process and may be conducted in accordance with the entity's Internal Audit or external assurance programs.

Pursuant to this Standard, conformity can ensure the plans, processes, procedures, teams, tools and equipment, facilities, and support needed to implement its response, incident management, communications, and business continuity plans were in place within the period when inspection and certification were carried out.
Certification of an entity's BC capability against a formal standard is no guarantee that it will be successful in managing disruption.
A.8.11.7 Compliance and Internal Audit
A.8.11.7.1 A formal BC Audit process should ensure the entity has an effective Business Continuity capability program. The purpose of a BC audit is to:

- Ensure compliance with the entity's BC policies and procedures;
- Review the entity's BC solutions;
- Verify the entity's BC plans;
- Verify that appropriate exercise and maintenance activities are available;
- Highlight deficiencies and compliance gaps;
- Ensure the remedy of such gaps.
- Audits should be conducted on a regular basis, as defined in the entity's audit and governance policies to ensure:
- Compliance with this standard;
- Consistency with BCM objectives and policy;
- Proper implementation, execution and sustainability; and
- Effective fulfillment of the entity's BCM capability objectives.

A.8.11.7.2 As regards BC, it is recommended that audit period should not exceed one year. In the interim, self-assessment and performance monitoring (through review of post-exercise and post-incident reports) may be carried out, if need be, by owners of the entity's BC plans, to ensure they remain fit for purpose. The current set of BC documentation that may be presented to those performing internal or external audits includes copies of the entity's:

- BC Policy
- BC roles, responsibilities and resources
- Progress reports of BC projects
- Training and competency records of BC personnel
- Output from a Business Impact Analysis, recovery and BC requirements analysis
- Threat assessments
- BC strategies including documentation supporting the choice of the strategies adopted
- Resource level support

- Incident response plans
- Incident management plans
- Business Continuity Plan
- Exercise program
- Exercise and test reports
- Awareness and training program
- Service level agreements with customers and suppliers
- Contracts for third-party recovery services such as workplace and leftovers
- Maintenance and review (audit) program, reports and corrective actions.
- Previous audit reports and corrective and preventive actions plan

A.8.11.7.3 Internal Audit procedures

To define audit scope:

1. Determine corporate governance, compliance and other issues to be audited.
2. Determine the locations, departments, and activities to be audited.
3. Define the audit approach:
4. Identify the auditing activities that will be undertaken, e.g. questionnaires, person-to-person interviews, document reviews and/or solution review.
5. Identify the audit activity timetable and due dates.
6. Identify the audit evaluation criteria (standards).
7. Determine audit requirements by specialists and experts, as a third party, to conduct audit process.

To review and gather information during audit activities:

1. Compile and summarize interview notes, questionnaires and other sources of evidence.
2. Identify gaps in content and level of information gathered; then conduct additional, or follow up, interviews as appropriate.
3. Obtain and compare relevant documentation, e.g. BIA with interview data and information from other sources such as walkthrough, physical inspection, or sampling.
4. Reference secondary sources e.g. standards, regulations, and good practice guidelines to validate preliminary findings.
5. Form an audit opinion that reflects the interests of the audit sponsor and the measurements set by external sources, e.g. regulatory, legal, or industry standards.
6. Define criteria to rate / weight audit findings
7. Assign a weight / rating to audit findings to identify whether they represent non-compliances of low, medium or high severity.

A.8.11.7.4 Internal Audit Report
To prepare the Internal Audit Report:
A (a) Provide a draft audit report for discussion with key stakeholders.
Provide an agreed-upon audit report incorporating recommendations as well as audit responses where differences of opinion appear.
Provide an agreed-upon remedial action plan including timescales to implement the recommendations set out in the audit report.
Identify a monitoring process, separate from the BC capability maintenance program, to ensure appropriate follow-up on the audit action plan.

A (b) the following should be reported to Top Management:
An independent BC audit report agreed-upon and approved by management
Remedial action plan(s) agreed and approved by Top Management

The outcome of an unfavorable rating should include:
Recognizing BC Plans by competent department as 'inadequate'.
Date of initiation of a BC review conducted by a BC professional to assist the entity in improving its rating.
The policy concerning the frequency of audit should be clearly defined and documented within the organization's Audit Policy and Standards.

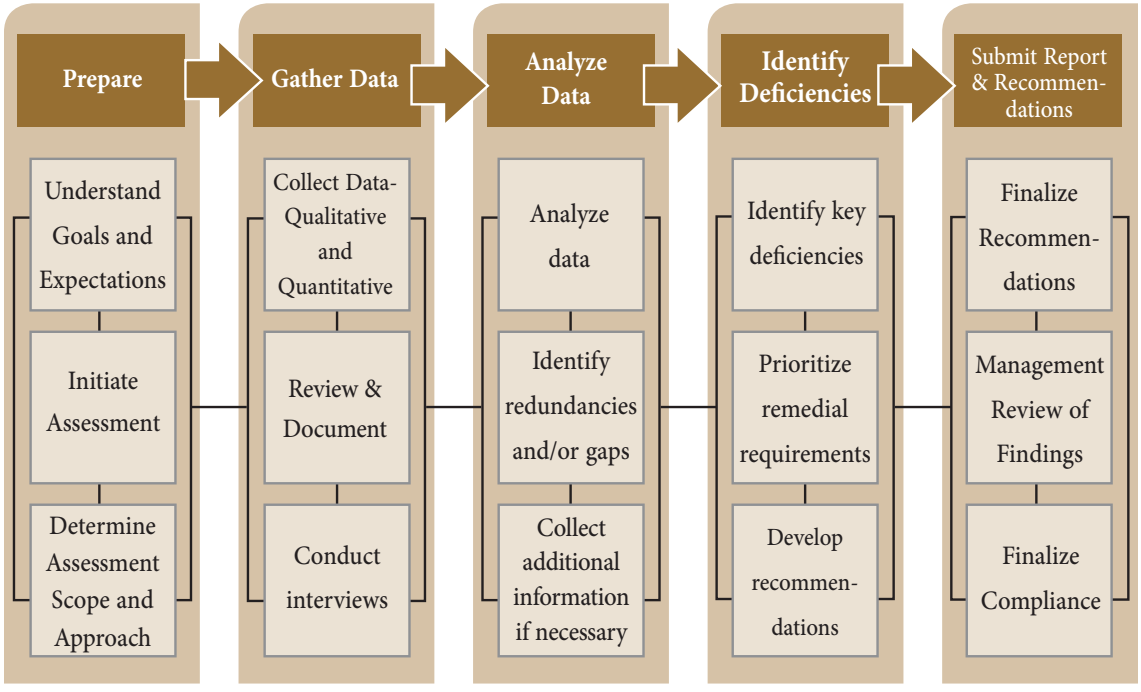
A.8.11.7.5 Corrections and Corrective Actions Plan
Once the audit report is submitted by the auditor, the auditor should develop a remedial plan called corrections and corrective actions plan.
A correction is an action to fix the known non-conformity.
A corrective action is an action to fix the cause of known non-conformity and prevent its re-occurrence.
Corrections and corrective actions should be within the capability of the entity.
Corrections and corrective actions may be maintained as a separate document or within the audit report.

A.9 BCM Assessment and Evaluation

A.9.1 Annual Review of the BC Capability

The Capability of the Business Continuity plans and infrastructure are required to be assessed at regular intervals and at least annually as part of the Certification process.

For further information, as part of the certification process, the formal Capability Assessment and Evaluation Certification will follow the process outlined below:



Certification process for assessment and evaluation of the BC capability

Certification involves providing evidence that the entity's BC plans, procedures and infrastructure will achieve its recovery objectives as defined in the BIA, identified in the BC Policy, and included in the scope of its BC program.

Where BC capability objectives are not met, an action plan should be developed to identify the steps required to achieve the objectives and monitor success in doing so.

The certification process sets sights on the entity's ability to ensure it has the proper mix of training, support, plans, human resources, leadership, equipment and facilities to meet its capability objectives during an emergency, crisis or disaster. This process involves a combination of impact scenario and function based planning, because it focuses on the entity's scenario-to-task-to-capability.

The certification process will require the entity to describe the process used to determine its capabilities and limits in preparing for, and responding to, an incident. The BIA and Risk Assessment should provide this core information and clear justification for the specifications of its recovery requirements.
The certification process will require the entity to show how its planned capabilities meet its recovery requirements, which options were considered in developing its BC Strategy, and why the strategy was chosen.

The primary method for proving the entity's BC Strategy is appropriate, as it ensures continuity of the critical activities identified in the BIA against threats identified in the risk assessment, and that its plans are fit for purpose is through exercising and testing those plans.

For this reason, the results of its exercises and tests are essential in documenting the entity's business continuity capability when it undergoes assessment for certification. The test plans and reports therefore make up some of the required documentary evidence at the time of certification.
(See 'BC Toolkit 1 – Templates' for test and exercise templates).

A.9.2 Review of Key Suppliers
As part of the annual review, an entity is expected to prove it has established the appropriate level of interaction with third parties and, particularly key suppliers. The steps taken to accomplish this interaction should include:

A.9.2.1 Reviewing the supplier's BC status and ensuring it is acceptable to the entity;
Integrating its Incident Management procedures with the supplier, to ensure there is a formal process for timely notification by either party in the event of a disruption;
Implementing acceptable levels of cost effective resilience into the business operations to mitigate failure of the third-party; and

A.9.2.2 Conducting exercises to evaluate and demonstrate the resilience of

the Third-party BC plans and capability, including suppliers or subsequent parties, to ensure their ability to continue delivering their services and meet their contractual obligations towards the entity. (See 'BC Toolkit 1 – Templates' for Supplier Questionnaire and Evaluation templates).

A.9.3 Review of Customers and Third Parties

Where the entity supplies products to customers and clients, its Incident Management and Business Continuity plans shall be reviewed based on the business objectives of the customers and clients, so as to ensure the entity can meet their expectations and fulfill the terms of its contracts and agreements with them, in accordance with the entity's BIA. This capability should also be checked through the previously mentioned exercises.

A.9.4 Post-Incident Review

All incidents of business disruption should be reviewed and analyzed to establish the level of impact, and to identify the cause as well as any corrective and preventative actions required. The results of this analysis should be recorded, summarized, and made available as part of the BC Capability Evaluation Report and should include:

- Nature and reason of emergency, crisis or disaster
- Assessment of management reaction in meeting the entity's BC objectives
- Assessment of entity's effectiveness in meeting BCM recovery objectives
- Identification of required changes to improve its BC capability

A.9.5 Annual BCM Evaluation Report should:

- Summarize the entity's prevention, protection, response, and recovery capabilities based on its plans, documentation of its tests of tools, equipment and infrastructure; and records of the training and exercise of its personnel;
- Describe the entity's key deficiencies and weaknesses;
- Describe the tests and exercises completed last year, including dates and results demonstrating proof of capability based on requirements and objectives;
- Make recommendations where improvements / remedial action is required to obtain certification;
- Include a plan of action with ownership assigned and date when each action should be completed;
- Detail any cost or budget required to achieve certification.
- The BC Capability Evaluation Report is required as documentary evidence for initial certification and annually during re-certification.

(See 'BC Toolkit 1 – Templates' for a BC Capability Evaluation Report template).

A.10 Management Review of Business Continuity Capability

A.10.1 Management Review

Management review involves assessment of improvement opportunities, and the need to apply changes to BC policy, as well as the performance goals, plans, operations, procedures, teams and support teams, to ensure they remain valid.

The management review should cover the scope of the entity's BC capability program. This review should be continuously scheduled and documented. In small-sized organizations, program elements may be reviewed all at once. In larger organizations, it may not be possible to do this and the review may take place over a period of time.

A.10.2 Management Review Documentation

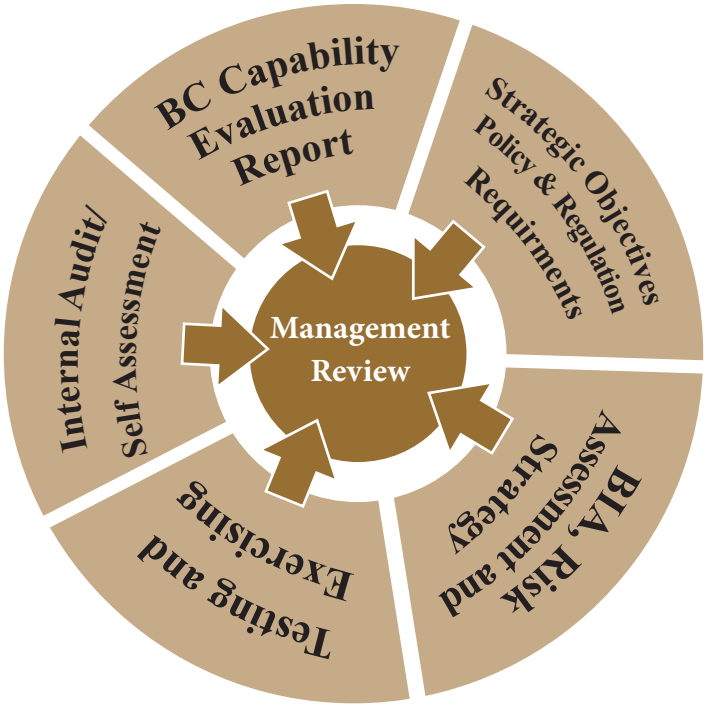
The Management Review may be conducted as part of the BC Capability Evaluation Review and the results recognized in the BC Capability Evaluation Report.

A.10.3 Management Review Input

The Management Review takes account of the:

- Strategic business objectives;
- Goals defined in its BC Policy;
- Risks identified in its Risk Assessment;
- Recovery objectives set out in its BIA;
- Strategy defined based on the above;
- Output from internal audit processes; and
- Results of plan testing and implementation.

In addition to Top Management, the BC capability review should involve persons who implement the entity's plans, such as the BC coordinators who are responsible for preparing its budget and monitoring its resources. This review should also include a review of the BC Capability Evaluation Report.



Business Continuity Management Review Process

In addition to the regularly scheduled management review, certain events can occur which may trigger a management review of the BC capability. These events include:

- Completion or revision of the entity's BC Policy, Risk Assessment, or BIA;
- Major changes to the entity's organization, its business objectives, business processes, facilities and IT hardware and software infrastructure;
- Changes in assumptions in the entity's Risk Assessment and BIA;
- Changes in the entity's Risk Appetite;
- Changes in the threats faced by the entity, including the environment, locations and markets it operates in;
- Changes in its suppliers and the supply chain;
- Major changes in the BC Standards or the continuity planning regulations and guidelines within the entity's business sector or industry:
- Revision of old requirements or addition of new regulatory and compliance requirements in the entity's sector or industry; and
- Latest events of disruption directly impacting the entity or similar organizations in the entity's sector or industry.

Where the disruption directly affects the entity itself, the management review should consider the reason of plan activation and success, etc.

Where disruption affects another entity, the management review should investigate the reasons behind the other entity's activation and determine whether the disruption or events that caused it affect the risk profile of the entity's own business.

A.10.4 Management Review Output

The output from a Management Review depends on whether it takes place as part of the BC Capability Evaluation or is done separately. If the management review was carried out as part of the entity's annual capability evaluation, the output should be contained in its BC Capability Evaluation Report. If the management review was, however, conducted separately, the output will be contained in a separate document identifying the:

- Scope of the review;
- Reasons for the review;
- People involved in the review;
- Areas where issues exist, highlighting any raised risks;
- Recommendations for corrective and preventative actions; and
- Brief review of tests and exercises.

This BC Management Review Report should serve as evidence for the entity's BC Capability Certification.

(See 'BC Toolkit 1 – Templates' for a BC Management Review Report template).

This report may be kept simple as the 'Minutes of the Meeting' (MoM).

Part 3:
BCM Toolkit

1 BC Plan Template

Disclaimer
The template has been developed by the Higher Council of National Security, National Emergency Crisis and Disaster Management Authority (NCEMA) for use by Entities in developing their incident management and business continuity plans.

In providing this template, NCEMA is not rendering legal or professional service in Incident Management or Business Continuity.

If legal or professional assistance is required, Entities are encouraged to seek the advice of a licensed or certified practitioner with appropriate training and professional experience.

Plan Information

Date Plan was created: _____

Date Plan was last updated: _____

Date Plan was last reviewed: _____

Date Plan was approved: _____

Name and Title of Approver: _____

Signature of Approver: _____

Entities may use this template as a guide to develop their Incident Management and Business Continuity Plan.
The template must be adapted as required to suit the entity's size and operations.

Plan Distribution List

This section provides contact details of all personnel and locations where copies of the plan are available.

A list of copyholders and locations where plan copies are retained is required to ensure that copies are controlled, valid and consistent with the latest reviews and updates.

If the list consists of more than 10-12 items, it may be included in an additional Annex.

Copy Number	NAME	Location
001		
002		
003		
004		
005		
006		
007		
008		
009		
010		
011		
012		

Introduction

The purpose of this plan is to support the Incident Management and Business Continuity activities required to meet an entity's business and regulatory requirements, as well as its contractual obligations and stakeholder expectations, following events which significantly disrupt its ability to operate.

This plan provides the information required to respond to an event, maintain continuity of main/essential activities, and provide the ability to return to normal operations.

Scope

This section of the plan identifies the entity's locations, sites and departments which are covered by the plan. Table rows are added where and when necessary.

Workplaces and functions covered by this plan include:

	Name and Address	Departments / Functions Covered
1		
2		
3		
4		
5		

Addressed Events and Scenarios

This section of the plan identifies the events and disruptions the plan is designed to address and handle.

At a minimum, the plan should address three assumptions:

- Loss of, or loss of access to, the main work site
- Loss of, or loss of access to, the computer applications and systems or technology infrastructure required for normal operations.
- Loss of human resources (including reduced capability)

According to the entity's risk assessment, take into account events and disruptions:

- Caused by nature - fires, flood, earthquakes etc…
- Caused by technology / system failure, power disruption, communications etc…
- Caused by man (man-induced): acts of sabotage, criminal acts by personnel inside or outside the organization and the impact of these acts on the entity's ability to meet its regulatory requirements, legal and contractual obligations and stakeholder expectations.
- In addition to events impacting a single building or location, Entities should also consider the events impacting a geographical area (e.g. loss of power, flooding, severe weather, etc.).

- These risks have been developed after conducting the entity's risk assessment or extracted from the risk register of the primary entity.

Objectives

This section of the plan provides an overview of the recovery objectives with respect to the entity's major departments or functional groups. These objectives are identified in the BIA.
This section should also identify the entity's planning assumptions.
Details of the recovery objectives and timeframes for all departments can be given in an Annex, if needed.
The objectives of this plan are to:

Team Preparation / Plan Invocation

This section of the plan explains the process for activating the entity's Incident Management and Business Continuity teams. It identifies the criteria, or 'triggers' that will be used to determine when the teams are activated and the plan itself is invoked.
This section also identifies which personnel have authority to invoke the Business Continuity plan.

Alert and Notification

This section of the plan explains the process for alerting the Incident Response Team that an event has occurred and for notifying internal and external stakeholders of the disruption resulting from such event, including people with special needs.

Teams / Groups

This section of the plan illustrates the hierarchy and structure of the entity's Incident Management and Business Continuity teams.

Roles and Responsibilities

This section of the plan identifies the primary and backup personnel who play key roles and lead the teams for incident response, damage and impact assessment, incident management, in addition to maintaining continuity of critical activities.
All persons listed in this section should review this table and the information

it contains to ensure they understand their role and assigned tasks.
The information in this section should be reviewed every 4-6 months to ensure it is up-to-date.
A list of roles commonly found in Incident Management and Business Continuity Teams is given below.

Core Team

- Incident Management Leader (appointed by Top Management);
- Business Continuity Manager;
- Information Technology representative;
- Facilities / Public Services representative (Communicates with **Damage Assessment team);**
- Communications / Media Relations representative;
- Scribe (to log minutes of meetings and decisions).

Support Team

- Human Resources representative;
- HSE representative; (if any)
- Security representative;
- Legal representative; and
- Operation and Business Support representatives.

Below is a model table clarifying roles and personnel entrusted with such roles and responsibilities.

Role	Primary	Alternate
Team Leader	Name: _____ Contact Information: 050-xxx-yyyy	Name: _____ Contact Information: 050-xxx-yyyy
Responsibilities: ensure the Plan has been activated oversee smooth implementation of the response section of the plan determine the need for and activate the use of an alternate sites liaise with key stakeholders as identified in Annex _____ provide Communication Team information for distribution to internal and external stakeholders inform key staff of changes and updates in the event and the entity's status.		

A complete list of key stakeholders should be listed in an Annex to this Plan.

Role	Primary	Alternate
Title	Name: Contact Details:	Name: Contact Details:

Role	Primary	Alternate
Title	Name: Contact Details:	Name: Contact Details:

Role	Primary	Alternate
Title	Name: Contact Details:	Name: Contact Details:

Evacuation and Assembly

If the entity fails to record its evacuation and gathering procedures in another plan, they should be recorded here.

The procedures should mention the steps to be taken to evacuate staff, visitors, and people with special needs from the building.

It should also identify the procedure of calculating the number of employees who were in the building.

Gathering areas should be identified in illustrative pictures, to indicate the place where building occupants should be heading after evacuating the building.

The evacuation section of a plan should:

- Provide a floor plan of the work place;
- Identify the location of emergency exits;
- List the steps to be taken during evacuation to provide assistance to persons with disabilities / special needs;
- State the acts to be performed by all building occupants if evacuation is deemed necessary; and
- Identify one or more gathering areas at a safe distance from the building.

Incident Response

This plan section lists the tasks to be fulfilled by entity's personnel before, during and after an emergency. It should be tailored to include information specific to the entity and its operations.

Incident response activities involve preparing and activating the entity's teams and plans to assess, manage and respond to, the incident impact, and recover from incidents which pose serious risks to the health and safety of its personnel and / or result in significant disruption of its critical functions and activities.

These disruptions include loss of primary work location, inability to perform main/essential tasks, and / or loss of vital infrastructure required to perform such tasks.

Activities in this phase include incident assessment and management and incident planning procedures, mobilization of teams and deployment of resources to respond to events causing, or having the potential to cause, immediate and serious harm to the entity's personnel, facilities, operations, and the communities where it operates.

Each member of the Incident Management Team is responsible for performing the following tasks and activities:

Pre-Event

- Get fully acquainted with the procedures of incident management and incident procedures planning, to be able to achieve the objectives of this plan.

During Event

- Ensure the health and safety of entity's personnel responding to and impacted by the incident, including people with special needs.
- Identify procedure strategies and plans of action for entity's response to, and recovery from, the incident.
- Ensure continuity of critical activities and services by available personnel or by personnel brought in where required.
- Lead teams in performing tasks assigned in the entity's incident action plans.
- Initiate communication with Incident Management Team and establish a centre of operations for the entity's incident command.
- Activate and operate alternative work areas and recovery sites as needed.
- Provide means of transportation for staff, equipment, data and supplies to alternative work areas and sites and determine whether such means of transportation are owned by the entity.

- Coordinate movement and accommodation (where required) at alternative work sites and recovery sites.
- Assist in identifying and tracking expenses and loss related to the incident as well as activities required for response and recovery from the incident.
- Arrange expenses and payment of invoices and find a disbursement mechanism without administrative or routine obstructions.

Post-event

- Extract information after the incident and submit a report on such incident including:
- Assess overall performance of teams during incident response;
- Assess overall effectiveness of the Incident Management and Business Continuity Plans;
- Assess overall effectiveness of the Incident Management and Business Continuity Teams in achieving the entity's emergency response objectives;
- Review results of incident information, post-incident report and feedback from teams involved in incident management, response and recovery.
- Issue recommendations for handling any issues that may arise in any of the aforementioned stages and the suggested solutions and lessons learned.

Warning and Notification

Warning and notification process involves four steps:

- Contacting the Core Incident Management Team.
- Assessing incident type and impact to determine whether to activate the Incident Management Support Team or not. This involves considering the incident type and scale and assessing current and potential impact. If such incident does not require activation of Incident Management Support Team(s), assigning personnel to monitor such event / situation and communicating with staff, where necessary.
- If such incident does not require activation of the Incident Management Support Teams, activating the Teams, as need may be, to respond to, and handle, such incident.
- Emergency Response, Initial Assessment and Incident Management

Team Activation

Upon activation, the Incident Management Team should:

Incident Management Team – Initial To-Do List		
	Activity/ What	**Responsibility/ Who**
1	Notify Police / Fire Emergency, if necessary if not already done).	First On Scene procedure
2	Conduct evacuations as necessary.	First responders
3	Notify the Incident Assessment Team.	First responders
4	Contact utility bodies to shut off power and gas, if need be.	Incident Management Team
5	Census of all personnel and visitors.	Incident Management Team and Zone Leaders
6	Identify injured and deceaded, as required.	First responders
7	Secure the location.	Incident Management Team and Zone Leaders
8	Determine extent of damage to buildings, work areas and IT/ Telecommunications systems.	IMT / Public Services / ICT
9	Determine impact of event upon ability to perform critical activities and support service.	Incident Management and Support Teams
10	Activate IMT Command Centre, where necessary.	Incident Management Team
11	Activate Alternative Work Sites, where necessary.	Incident Management Team
12	Identify stakeholders. Determine communication, messaging and information strategy required by internal and external stakeholders.	Incident Management Team / Communications

Emergency Response and Impact Assessment involves use of the Core Incident Management Team to determine impact of the event on:

- Health and safety of personnel
- Buildings, facilities and work areas
- Infrastructure needed to support critical activities (e.g. ICT, Power, Water, Gas)
- Ability to conduct business critical activities
- Ability to communicate with internal and external stakeholders

Incident Communication

If the entity fails to record its communication procedures in another plan, such procedures should be recorded here.

The Communications Plan should include the following:

- Categories of Emergency Operations
- Audiences, Types of Information, and Required Messages
- Roles and Responsibilities for Developing and Delivering Messages
- Communications Officer
- Communications Team
- Communication and Messages needed for three scenarios at least:
  - Emergency Operations - Reduced Ability to Perform Main/Essential Functions and Activities at One or More Locations
  - Suspended Operations – Inability to Perform Main/Essential Functions and Activities at all locations
  - Return to Normal Operation - Ability to Resume Main/Essential Functions and Activities at All Locations

Continuity

Main / Essential Functions / Business Continuity Task Lists

This section of the plan identifies the entity's critical activities and the actions taken to maintain continuity.

Each department should develop a Business Continuity Task List for the continuity of its critical activities.

BIA should be used to identify the critical activities.

The table below can be used to develop Business Continuity Task Checklists.

Business Continuity Task List

Main / Essential essential Activities / functions	Recovery Requirements	Resource Requirements	Timeframe	Responsibility	Completed

The table in this section should be developed, taking into consideration maintaining business continuity in a 'worst- case' scenario. It can then be modified to match less severe disruption of the entity's operations.

During Incident Management, this table can act as a checklist when the last column can be maintained (activity completion status).

Recovery

Recovery means return to normal operations.
The table in this section of the plan should be completed, taking into account supporting recovery in a 'worst case' scenario. It can then be modified to match the level of disruption to the entity's operations.
Recovery process includes:

Identifying resources required to resume these activities

Mentioning the persons responsible for each task and the expected completion date.

The table below can be used to develop the Recovery Action Task Lists.

Recovery Action Task List

Main / Essential essential Activities / functions	Recovery Requirements	Resource Requirements	Timeframe	Responsibility	Completed

Plan Exercise and Update

Training

At some point, it is necessary to receive required training on a certain plan, to ensure its validity and usefulness. This training can be carried out in the form of a practical exercise or simulation.

It also gives personnel implementing the plan an opportunity to get acquainted with such plan and their roles and responsibilities in implementing it, which is paramount for the success of such plan. To that end, the plan should include a training program for all personnel who may be involved in an emergency at the site, including people with special needs.

The schedule should list the team members and specify their title and role

Update

It is also critical that a plan be reviewed and updated periodically, to ensure its consistency with changes to the entity's organizational structure, operations, personnel, suppliers and contractors.

In addition, after an exercise or activation, the plan shall be reviewed and updated by the team(s) to include information on how useful the plan was in accomplishing the entity's objectives.

Details of plan review and update can be logged in a table like the one shown below.

Review Date	Reason for Review	Changes Made

Annex A - Key Contacts

Internal Key Contacts

Use this table to list emergency contact details of the members of Incident Management and Business Continuity team(s).

Person	Contact Number(s)	Email	Responsibilities

This table should also identify the backup resources and their contat details.

External Key Contacts
Use this table to document external services (including Emergency Services) contact details.

Key Contacts	Contact Number(s)
Ambulance	
Hospital	
Medical Services	
Fire	
Police	
Electricity	
Emergency Services	
Gas	
Insurance company	
Security	
Sewage	
Suppliers	
Telecommunication Company	
Waste Disposal	
Water	
Water	

Annex B - 'GO PACK' (aka 'Emergency Box')

When the main site is damaged or shall be evacuated and the entity has to transfer its operations to an alternative site, a "GO PACK" or emergency box should be prepared for each work group, to ensure it can perform its significant activities.
The "Go Pack" should be stored in a location where it can be easily accessed or in a safe and secure location away from the main site.

Note:
Make sure the "Go Pack" is safely and securely stored on-site or off-site (in another location).
Ensure "Go Pack" items are regularly checked, updated, and in a good working condition.
Remember that cash/credit cards may be needed for emergency expenditure.
Items to consider including in the "Go PACK" are listed below. The list should be modified to suit the entity and its needs.

Documents
- Site plan, including location of gas, electricity and water shut off points (preferably laminated).
- Business Continuity Plan
- Contact details of emergency services and local authorities.
- Contact details of employees – including home and mobile phone numbers and e-mail addresses. It is also preferred to include contact information of staff relatives.
- Contact details of key customers and suppliers.
- Contact details of utility companies.
- Contact information and details of insurance coverage firms.
- Engineering plans and drawings.
- Evacuation plan.
- Financial and banking data.
- Curriculum and trade secrets.
- Latest inventory of supplies, stock and equipment (on a permanent basis).
- Product and specification lists.
- Stationery with letterhead, company seals and documents.

Equipment
- Computer back-up media / disks / USB memory sticks or flash drives.
- Disposable cameras (for recording evidence in an insurance claim)

- Dust and toxic fume masks.
- General stationery (pens, paper, etc.).
- Hazard and cordon tape.
- Loud Hailer (batteries to be kept sealed until used)
- Marker pens (for temporary signs).
- Message pads and flip chart paper.
- Mobile telephone with credit available, plus charger.
- Radio (batteries to be kept sealed until used) – consider wind up type
- Small toolkit (hammer, wrench, screwdriver and spanner set)
- Spare keys
- Torch - consider wind up type.
- Voice recorder

Note: Damageable stuff such as batteries and films should be recycled.

Supplies
- Batteries for Emergency Box items (sets)
- Hard Hats (Helmets)
- Rolls of Hazard Tape
- Thick Gloves (Pairs)

Annex C - Sample Reports & Forms

A number of forms, reports and guideline manual shall be available with the entity's Incident Management and Business Continuity Teams. These forms and reports include:
- Instructions on how to record and update messages, using the entity's voice-mail system.
- Sample message scripts for incident notification
- Sample message scripts for announcement of relocation to alternative work site (e.g. notification to internal and external stakeholders)
- Equipment damage report
- Facility damage report
- Expense report
- Problem tracking form (for alternative work site)
- End-of-day status report to Top Management
- Repair / restoration at main site
- Continuity of critical activities / works at alternative work site
- Incident Report
- Date/time of event

- Location of business impact
- Incident description
- List of buildings, facilities, work areas affected by such incident
- Description of incident impact on business operations and critical activities
- Current Status
- Event log
- Sample (Event Log)

This form can be used to record information, decisions and actions during the period immediately following the incident and the days that follow until the Incident Management and Business Continuity Teams are de-activated.

Date	Time	Information / Decisions / Actions	Signature/ Initials

Annex D – References and Related Documents

This section includes the documents that contain additional information required to implement this plan.

Document Title

Alternate Work Area Locations and Information

Location of the Incident Management Command Centre, along with contact information and list of available equipment there - Locations of Main workplaces/ Alternative Emergency sites/ Gathering Areas, along with procedures for building evacuation and census of employees
Locations of Alternative Work Sites of all departments, along with telephone numbers and maps of each location

Wallet Card

- Emergency Hotline Number
- Emergency Assembly Area location
- Command Centre location and phone number
- Alternate work location and phone number
- Information for Key Contacts

24-hour Contact Lists

- Internal and external emergency services
- Key personnel
- Employee call tree
- Customers
- Incident Management and Business Continuity Team Leaders (primary / alternate)
- Incident Management and Business Continuity Team Members
- Third-Parties providing disaster recovery services

Contact Numbers

- Work
- Phone number
- Alternate phone number
- Fax number
- Home
- Mobile

Annex E – Glossary

Term	Definition
Activity	process or set of processes undertaken by an organization (or on its behalf) that produces or supports one or more products or services
Audit	systematic examination to determine whether activities and related results conform to planned arrangements and whether these arrangements are implemented effectively and are suitable for achieving the organization's policy and objectives
Business continuity	strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level
Business continuity management (BCM)	holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities
Business continuity management lifecycle	series of business continuity activities which collectively cover all aspects and phases of the business continuity management programme
Business continuity management personnel	those assigned responsibilities defined in the BCMS, those accountable for BCM policy and its implementation, those who implement and maintain the BCMS, those who use or invoke the business continuity and incident management plans, and those with authority during an incident
Business continuity management programme	ongoing management and governance process supported by top management and appropriately resourced to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products and services through training, exercising, maintenance and review

Term	Definition
Business continuity management response	element of BCM concerned with the development and implementation of appropriate plans and arrangements to ensure continuity of critical activities, and the management of an incident
business continuity management system	that part of the overall management system that establishes, implements, operates,monitors, reviews, maintains and improves business continuity
business continuity plan (BCP)	documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical activities at an acceptable pre-defined level
business continuity strategy	approach by an organization that will ensure its recovery and continuity in the face ofa disaster or other major incident or business disruption
business impact analysis	process of analysing business functions and the effect that a business disruption might have upon them
consequence	outcome of an incident that will have an impact on an organization's objectives
cost-benefit analysis	financial technique that measures the cost of implementing a particular solution and compares this with the benefit delivered by that solution
critical activities	those activities which have to be performed in order to deliver the key products and services which enable an organization to meet its most important and time-sensitive objectives
disruption	event, whether anticipated (e.g. a labour strike or hurricane) or unanticipated (e.g. a blackout or earthquake), which causes an unplanned, negative deviation from the expected delivery of products or services according to the organization's objectives
exercise	activity in which the business continuity plan(s) is rehearsed in part or in whole to ensure that the plan(s) contains the appropriate information and produces the desired result when put into effect

Term	Definition
gain	positive consequence
impact	evaluated consequence of a particular outcome
incident	situation that might be, or could lead to, a business disruption, loss, emergency or crisis
incident management plan (IMP)	clearly defined and documented plan of action for use at the time of an incident, typically covering the key personnel, resources, services and actions needed to implement the incident management process
internal audit	audit conducted by, or on behalf of, the organization itself for management review and other internal purposes, and which might form the basis for an organization's selfdeclaration of conformity
invocation	act of declaring that an organization's business continuity plan needs to be put into effect in order to continue delivery of key products or services
likelihood	chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies or mathematical probabilities
loss	negative consequence
management system	system to establish policy and objectives and to achieve those objectives
maximum tolerable period of disruption	duration after which an organization's viability will be irrevocably threatened if product and service delivery cannot be resumed
nonconformity	non-fulfilment of a requirement
organization	group of people and facilities with an arrangement of responsibilities, authorities and relationships
process	set of interrelated or interacting activities which transforms inputs into outputs

Term	Definition
products and services	beneficial outcomes provided by an organization to its customers, recipients and stakeholders, e.g. manufactured items, car insurance, regulatory compliance and community nursing
recovery time objective	target time set for resumption of product, service or activity delivery after an incident
resilience	ability of an organization to resist being affected by an incident
resources	all assets, people, skills, information, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that an organization has to have available to use, when needed, in order to operate and meet its objectives
risk	something that might happen and its effect(s) on the achievement of objectives
risk assessment	overall process of risk identification, analysis and evaluation
risk management	structured development and application of management culture, policy, procedures and practices to the tasks of identifying, analysing, evaluating, and controlling responding to risk
stakeholders	those with a vested interest in an organization's achievements
system	set of interrelated or interacting elements
top management	person or group of people who direct and control an organization at the highest level

For additional information and for guidance, Please contact NCEMA at:

Safety and Prevention Department, Business Continuity Section
Tel : 02 / 417 7000 - 02 / 4177020
E-mail: info@ncema.gov.ae