UNITED ARAB EMIRATES الإمـارات الـعـربية المتحدة

الـمجـلـس الأعـلى للأمن الـوطـني

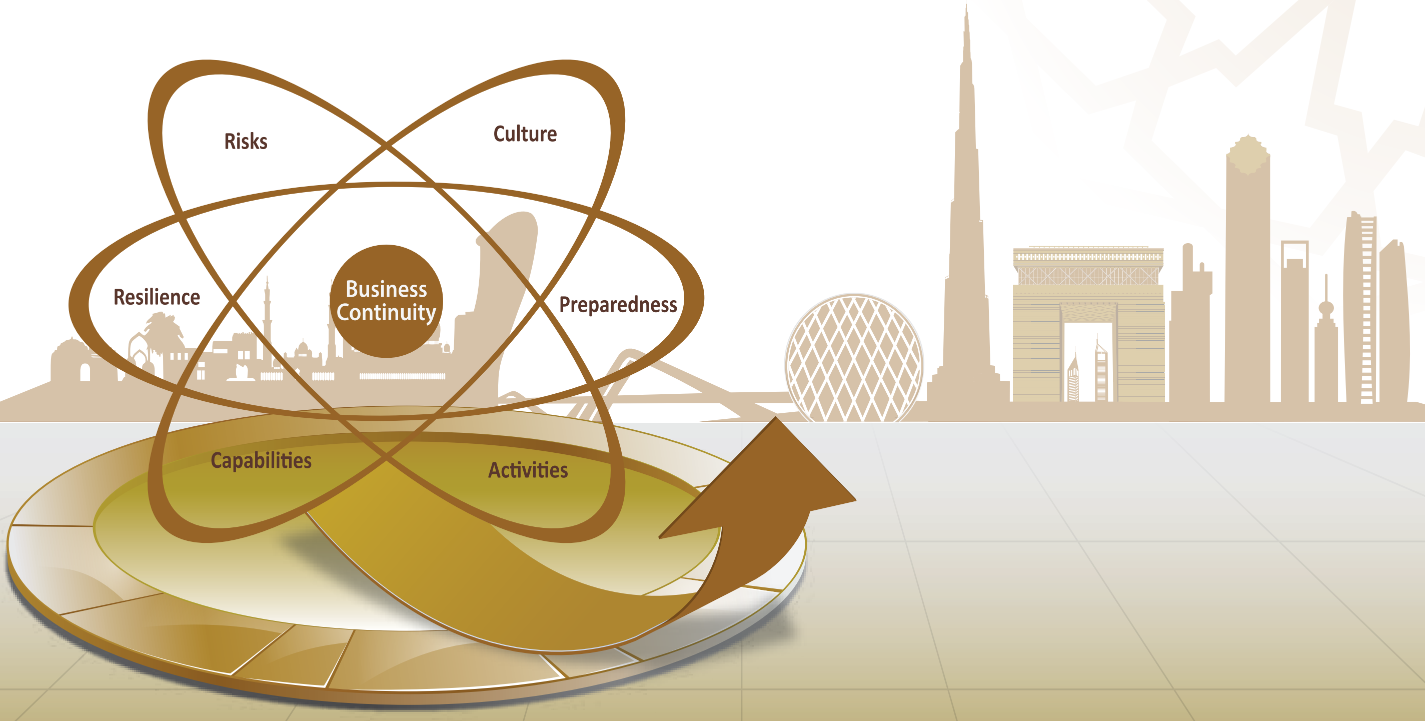
THE SUPREME COUNCIL FOR NATIONAL SECURITY

الهيئة الـوطنيـة لإدارة الطوارئ والأزمـات والكـوارث

National Emergency Crisis and Disasters Management Authority

BUSINESS CONTINUITY MANAGEMENT STANDARD

(GUIDELINES)



AE/SCNS/NCEMA 7001:2015

BUSINESS CONTINUITY MANAGEMENT STANDARD

(GUIDELINES)

AE/SCNS/NCEMA 7001:2015

The Supreme Council for National Security
National Emergency Crisis and Disasters Management Authority
Approved by National Media Council, Abu Dhabi, UAE (2015/30184)

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

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

Business Continuity Management Standard Guidelines
AE/SCNS/NCEMA 7001:2015

Use Key

NCEMA Provides a Business Continuity Management Standard to build an organization’s capability to continue functioning and delivering its prioritized activities when its operations are disrupted die to emergencies or crises. The standard consists of three major parts provided in separate publications and are available on NCEMA website.

Specifications

Which the Business Continuity Management Standard – Specifications (AE/SCNS/NCEMA 7000:2015).

Guidelines

(AE/SCNS/NCEMA 7001:2015)

The purpose of this document, which interprets “how” the elements mentioned in the “Specifications” work. The sections in “Guidelines” reflect their counterparts in the “Specifications”, bearing the same numbering system. For example, clause 4 in “Specifications” corresponds to clause A-4 in “Guidelines”, etc.

Toolkit

Includes BCM framework templates

This document does not contradict with any other document issued by the National Emergency Crisis and Disasters Management Authority (NCEMA). In case of contradiction, please refer to the documents concerned and follow them. This document is “Guidelines” and is only to manage business continuity.

Preface

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

Due to the development in the Business Continuity Management field, the second version of the Business Continuity Management Standard – Specifications (AE/SCNS/NCEMA 7000:2015) was officially released in 2015, along with the development of the second version of these Guidelines by a professional team from NCEMA and participation from experts and professional bodies and strategic partners.

Bodies participating in the specialized review of the Guidelines:

- Abu Dhabi Investment Authority
- Emirates Nuclear Energy Corporation (ENEC)
- Finance Department – Government of Sharjah
- Abu Dhabi Polymers Company (Borouge)
- Abu Dhabi National Bank
- DNV-GL
- Ventures Middle East

Table of Contents

Use Key 01

Preface 02

Introduction 05

Definitions 08

A-1. General 12

1.1. Purpose 12

1.2. Responsibilities 12

1.3. Controls set by Legislative Bodies 13

1.4. Plans and Procedures 13

A-2. Applicability 13

A-3. Responsibility Level 14

A-4. Scope 14

4.1. Scope of the Guideline 14

4.2. Organization’s Scope of Business Continuity Capability 15

A-5. Business Continuity Program establishment 16

5.1. Understanding the organization 17

5.2. Top Management Commitment 18

A-6. Business Continuity Capability 22

A-7. BCM Documentation and Records 22

7.1. Required Documents 22

7.2. Controlling BCM documentation and record 23

A-8. Business Continuity Managements Program Operations 25

8.1. Business Impact Analysis 27

8.2. Risk Assessment 30

8.3. Business Continuity (BC) Strategies 39

8.4. Incident Response Plan 48

8.5. Business Continuity Plan (BCP) 50

8.6. Media Response plan 52

8.7. Awareness and training 54

8.8. Test and Exercise 56

A-9. Business Continuity Program Review 60

9.1. Annual Review 60

9.2. Review of Suppliers and Service providers 62

9.3. Compliance and Internal Audit Review 63

A-10. Top Management Review 66

10.1. Management review of BCM Program 67

10.2. Documentation of the management review 67

10.3. Points of input during management review 67

10.4. Management Review outcome 67

A-11. BCM Program Continual Improvement 68

11.1. Non-Conformities 68

11.2. Corrective Actions 69

Right of Use 71

Contact NCEMA 71

Introduction

Under the guidance and directions of the wise leadership and the UAE federal government which continuously strives 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 Disasters Management Authority (NCEMA) drafted the first version of Business Continuity Management Standard and Guidelines in 2012.

This Guidelines document has been developed to adapt international best practices in business continuity management. This UAE Business Continuity Management Standard Specifications and Guidelines along with templates are unique in the sense that they are provided together comprehensively.

These BCM Guidelines have been developed to assist organizations systemically build their business continuity capability before, during and after an emergency, disaster or crisis. All these initiatives are aimed at ensuring ongoing performance of prioritized activates in both public and private sectors, for the purpose of enhancing the UAE's national stability.

Government organizations and its private sector partners should effectively handle emergencies and crises in a well-coordinated manner in order to fully recover from such situations. Service delivery should be maintained at minimum required level and should not be disrupted when an emergency occurs until recovery is complete.

The following Business Continuity Management documents and references have been used:

- International Standard ISO 22313:2012 – Societal Security – Business Continuity Management Systems – Guidance
- International Standard ISO 31000:2009 - Risk Management – Principles and Guidelines
- British Standard BS 25999-1:2006 Business Continuity Management – Specifications
- BCI Good Practice Guidelines 2013 from Business Continuity Institute

The information was tailored to match the nature of the UAE government business. It provides the international best practices used by internal and external parties to help organizations continue performing their prioritized activities, comply with their organizational and contractual commitments and to protect the interests of beneficiary organizations after an emergency, crisis or disaster that hinders the organization from properly performing is activities and services. The Guidelines can be applied to different sized organizations, in both public and private sectors.

Guidelines

Definitions

Term	Definition
Activity	A process, service, procedure, product, task, or combination of them that are managed by organization.
Audit	An organized, autonomous and documented form of activity of an organization conducted by an independent body in order to comply to the BCM Standard
Awareness	Development of understanding of primary Business Continuity Management risks and issues. Awareness enables the workforce to identify threats and responding promptly and appropriately. Awareness is created among employees in the organization and it is less formalized as compare to training.
Business Continuity (BC)	The ability of the organization to continue its prioritized activities at predetermined level after the occurrence of disruptive incident.
Business Continuity Management (BCM)	A comprehensive management process, which highlights possible threats and impact of such threats on business operations of the organization. The identification of threats assists to develop organizational resilience, toward these threats, and an effective and suitable response that will protect the stakeholders' interest, brand name and reputation.
Business Continuity Management Program (BCM Program)	It is a component of overall organizational management system, which establishes, implements, operates, reviews, monitors, maintains and improves business continuity capability.
Business Continuity Plan	Set of procedures in a documented form, which direct the organization to react, recover, restore and restart the predetermined level of operations after the interruption.
Business Continuity Policy	It is the major document that identifies the governance and scope of business continuity plan along with BCM objectives and highlights the cause of its implementation.
Business Continuity Strategy	The method of an organization to plan in order to recover and continue after a disruptive event.
Business Impact Analysis (BIA)	It is the process for analyzing business activities and the impacts of disruptive incidents that may happen over time.
Competence	Capacity to apply skills, resources and knowledge to accomplish desired goals.
Continual Improvement	Consistent activities to increase the performance level.
Compliance	Extent to which requirements are fulfilled

Term	Definition
Conformity	Extent to which mandatory requirements are fulfilled.
Corrective Action	Steps or measures that remove discrepancies.
Capability	Ability of capacity to perform a specific activity effectively.
Disruption	An incident which disturbs routine operation, process or function of the business. These events could be anticipated or unanticipated.
Exercise	Activity in which the business continuity plans is rehearsed in a part or in whole to ensure that the plans contain the appropriate information and produce the desired results when put into effect.
External and internal issues	External or internal variables that can have impact over the business continuity capability of the organization.
Fit-For-Purpose	Fulfilling the requirements of the organization.
Interested Party	Individual, group, or an organization which can affect or be affected or consider to be influenced by an activity or decision.
Incident Response Plan	Set of procedure for immediate response after an accident, and it is focused upon the safety of personal
Internal Audit	A compliance review against BCM standard requirements. Therefore take corrective actions and suitable decisions accordingly.
Minimum Business Continuity Objective (MBCO)	Minimal level for product or service, which considered as appropriate for the organization to accomplish organizational goals after disruption
Media Response Plan	Set of procedures that will enable organization to communicate with media and interested parties throughout roles and responsibilities and use of available media channels to communicate and deliver the necessary information and instruction effectively during a disruption.
Maximum Acceptable Outage (MAO)	Time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable.
Non Conformities	Mandatory requirements in the BCM standard not fulfilled.
BCM Objectives	The targets or goals that an organization wants to achieve throughout the BCM Program.

Term	Definition
Prioritized Activities	Activities that are critical and must be given priority when recovering from a disruptive incident in order to reduce the impacts
Process	It is a set of interdependent actions that convert inputs into finished products
Resources	Resources include information, skills, people, technology, assets and premises, which are obtain and used by an organization to achieve its organizational goals and objective.
Recovery	Retrieval or recapturing of normal or prior state.
Recovery Strategies	A strategy that is used by an organization to make sure it's regaining or continuing after an incident.
Risk Appetite	The extent to which an organization can afford and bear the risks and neutralize these risks to eliminate the threats.
Recovery Time Objective (RTO)	Time span after the occurrence of an incident in which an activity or product should be restarted or resources and assets should be regained.
Risk Assessment	The process in which risks is identified, analyzed and evaluated.
Risk	The impacts of uncertainties on organizational goals.
Stand Down	An official declaration, which communicates that emergency situation is controlled and no further invocation of plans is required.
Top Management	Group of individuals sitting at the top of the organization and plays the role to guide and control the organization.
Test	This is an activity or action that is undertaken to gauge the capabilities or effectiveness of a strategy or plan against a predetermined criteria or benchmark.
Training	This activity is more formalized as compared to awareness. It purports to build skills and knowledge to increase the performance of staff regarding a specific function.
SMART Objectives	Specific, Measurable, Achievable, Relevant and Times objectives.

Business Continuity Management Action Model

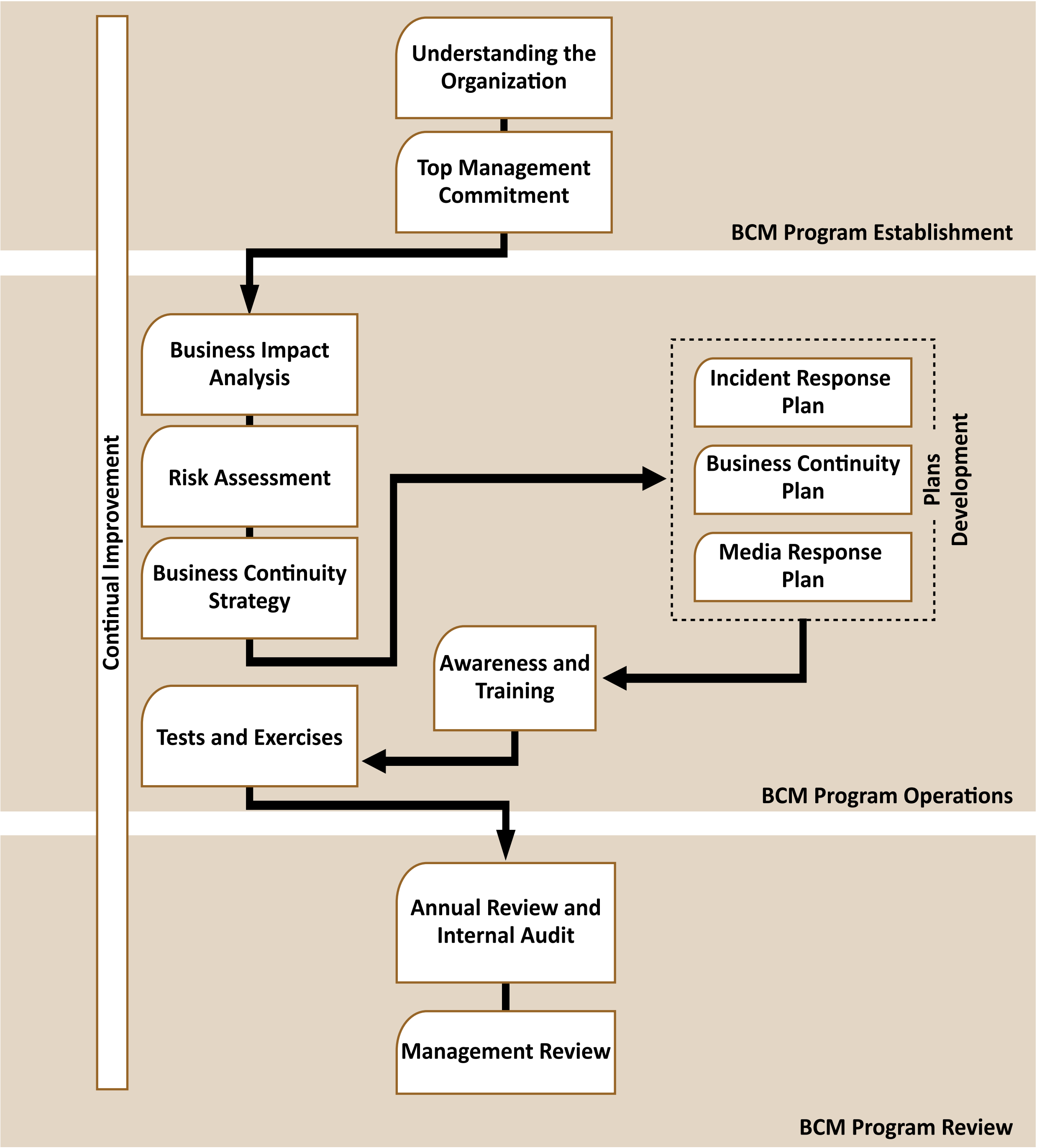


Figure 1: BCM Action Model

A-1. General

1.1. Purpose

This document is aimed at providing a common set of guidelines that can serve the purpose in referencing to the development, implementation, establishing and maintaining a BCM (Business Continuity Management) Program by all the public and private sectors across the nation. As a body of knowledge, this document main emphasis is laid on providing help for following:

a. Enlist prioritized activities based on the understanding of the strategy, objectives and culture of the organization;
b. Analyze and evaluate the impact on prioritized activities in case of a disruption;
c. Analyze the risks involved and their impacts on business disruption;
d. Develop the Business Continuity (BC) Capability of the organization with the intention of responding and recovering from the disruptions;
e. Develop an integrated and coordinated set of plans for increasing organization resilience;
f. Validate the BCM Program by conducting exercises, maintaining and continually reviewing for improvement.

1.2. Responsibilities

Refer to AE/SCNS/NCEMA 7000:2015 specifications Figure 2.
NCEMA is committed and dedicated in establishing the guidelines for the BCM Program.

1.3. Controls set by Legislative Bodies

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

1.4. Plans and Procedures

Based on the nature, size and complexity of activities, an organization should develop their BCM Program. Top Management in an organization should approve the details and level of the plans to be maintained, whether to have individual business continuity plan, disaster recovery plans, crisis & incident management plans and emergency response plans. For ease of planning, implementation and maintenance organizations may combine two or more of these plans.

A-2. Applicability

The requirements and specifications set forth in this BCM standard are general and are applicable to all types of organizations irrespective of the sector they belong to. Every organization should assume the responsibility of defining and documenting its “fit for purpose” BC Capability, which ensures performance of prioritized activities and services during disruptive incidents. Pursuant to this BCM standard, organizations should identify their prioritized activities as well as the business units, departments and sections where such activities are performed. In addition, organizations should identify their associates such as third-party suppliers, service providers and partners which provision goods and services needed to perform these activities.

A-3. Responsibility Level

The Top Management remains the decisive body and the driving force that endorses the success of the implementation of a BCM Program within the organization. Top Management should provide their leadership, commitment and all the resources required to implement and validate the BCM Program. Moreover, the commitment and support of Top Management is required not only during the initiation of the BCM Program but also during the entire implementation of the BCM Program.

Top Management can evident their commitment by:

- Understanding their role in the BCM Program and communicating the importance of BC in the organization
- Ensuring the availability of resources required to implement the BCM Program
- Conducting periodic management reviews.

Top Management can define appropriate competencies and responsibilities to other levels in order to implement the BCM Program. This standard, along with these guidelines, offers the minimum requirements needed for a BCM Program.

A-4. Scope

4.1. Scope of the Guideline

These guidelines are applicable to all the types and sizes of organization that wish to develop, implement, operate, maintain, review and continue its prioritized activities following an emergency, crisis or a disruptive incident.

4.1.1. This guideline should not be used to assess an organization’s ability to meet its own business continuity needs, nor any customer, legal or regulatory needs. Organizations wishing to do so should use the “Business

Continuity Management Standard – Specifications AE/SCNS/NCEMA 7000:2015" to demonstrate conformance to others.

4.2. Organization's Scope of Business Continuity Capability

Importance and purpose of setting out the scope

The determination of the scope of the BCM Program is of utmost importance before its implementation and deployment. The main objective of setting the scope of a BCM Program is mainly aimed at ensuring transparency of what areas of the organization are included and what areas are excluded within the scope of BCM Program. A thorough study and comprehensive understanding of the objectives, strategies and culture of the organization must be ensured before setting the scope. The scope comprehensively defines the activities, products and services, locations, functions, and processes to which the BCM Program applies.

4.2.1. Organization should define the deliverables, outputs, activities, services and functions that fall within the scope of its business continuity capability.

Process of setting out the scope

While setting out the scope, intensive study, and comprehensive understanding of the strategy, objectives and culture of the organizations is very essential. Setting up the scope of the BCM Program lies within the jurisdiction of the Top Management in order to define specific and explicit areas of the organization regarding their inclusion within the BCM Program. Once the scope has been determined, the organization should communicate it to interested parties.

Factors to consider when setting out the scope:

- Scale: The nature, size, and the complexity of the organization
- Risk: The organizations risk appetite

- BCM Maturity: What level of BCM Program maturity does the organization currently possess
- Geographical Location: Locations, facilities, and environment
- Governments directives, standards, regulatory or legal requirements shall be fulfilled.

4.2.2. The organization's scope for business continuity should include all activities required to maintain its prioritized activities**.**

The scope document should identify but not be limited to:

- Agreed-upon objectives and business priorities;
- The deliverables required during the project and delivery times of primary and final products;
- Any assumptions whereby risk or impact statements can be provided;
- Locations and / or activities to be included in or excluded;
- The organizational structure of the organization's BCM Program (roles and responsibilities).

A-5. Business Continuity Program establishment

Top Management is responsible for the establishment of the BCM Program and may appoint a BC Manager or Head of BC. The BC Manager or Head of BC is responsible for implementation and maintaining the BCM Program.

Depending on the size of the organization, it may be a full or part-time duty. To emphasize the importance of duties and responsibilities associated with the BCM 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.

5.1. Understanding the organization

The primary purpose of a BCM Program is to enable the organization to promptly and effectively respond to business disruption and maintain continuity of its prioritized activities, taking into account all interested parties involved in performing prioritized activities.

5.1.1. Identify all processes, relations, partnership, and supply chains with interested parties.
5.1.2. The overall risk which the organization is willing to undertake.
5.1.3. While implementing the BCM Program certain external and internal issues may affect the desired outcomes of the BCM Program.

Internal issues are factors that occur within an organization such as:

- Organizations financial changes
- Changes in the Top Management
- Employee morale
- Change in the culture of the organization

External issues are factors that take place outside the organization and are harder to predict and control, such as:

- Changes to the economy
- Threats from competition
- Political factors
- Government regulations
- The industry itself

5.1.4. Identify the needs and expectations of the addressed interested parties and their legal and regulatory requirements. 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.

5.2. Top Management Commitment

Commitment from the Top Management is one of the main factors for a successful implementation the BCM Program.

5.2.1. Top Managements commitments should be evidenced through:

- Establishing a BC Policy and Objectives
- Ensuring the BCM Objectives are met
- Assigning roles and responsibilities
- allocating the resources for implementing the BCM Program
- Actively participating in selection of the BC Strategy
- Actively engaged in exercising and testing
- Ensuring internal BCM Programs audits are conducted
- Conducting effective management reviews of the BCM Program
- Directing and supporting improvement of BCM Program.

5.2.2. Top Management should ensure that the organization's BCM objectives are identified. The BCM Objectives should:

- Be aligned with the organizational strategic objectives
- Determine Minimum Business Continuity Objective (MBCO)
- SMART and be set as a performance indicator in the BCM Program.

5.2.3. Business Continuity Policy shall be approved by the Top Management. The policy shall include BCM objectives and risk appetite, and be published internally and to interested parties (If applicable).

5.2.4. Refer to AE/SCNS/NCEMA 7000:2015 Specifications Clause 5.2.4.

5.2.5. The responsibility of the Top Management is to assign qualified experienced personnel to implement, maintain and continually improve the BCM Program. Assigned personnel should receive relevant trainings to fulfill their responsibilities in maintaining and operating the organization's BCM Program.

5.2.6. Different members from each department of the organization maybe identified to assist in the implementation of the BCM Program depending on the size and complexity of the organization. Their BCM roles and responsibilities may be collaborated with their daily jobs. The minimum required roles and responsibilities of the Business Continuity Management team who would be accountable and responsible to establish, implement, operate and maintain the BCM Program detailed as below:

BCM Manager

- Establish and demonstrate commitment to BCM Policy
- Responsible for all BCM Program activities
- Nominate the BCM team with appropriate seniority and authority that is accountable for BC Policy and implementation
- Facilitate approval of all BC plans, exercises and strategies
- Raise recommendations of BCM Team and BCM representatives during management review meetings

Incident Response Manager

- Participate in the development of the Incident Response Plan
- Ensure that Incident Response Plan is regularly updated
- Ensure safety procedures for all resources including personnel during a crisis
- Raise incident response awareness to staff across the organization
- Be the main point of contact between the incident response teams
- Progress updates on damage assessment
- Manage the incident response process

BCM Team

- Accountable to establish, implement, operate and maintain the BCM Program.
- Overall responsibility for the maintenance of the BCM documentation for any improvements in the BCM Program.
- Ensure conduct of reviews on all aspects for the BCM Program.
- Assess preparedness of different departments for meeting the recovery strategies and BCM objectives.
- Organize and coordinate the BCM awareness programs.
- Create the annual exercise program and seek approval from appropriate authority and distribute it to all concerned stakeholders of the BCM Program.
- To ensure BCM exercises, internal audits if any and management reviews are carried out periodically.
- Maintain relation with departments and liaise with various departments during crisis.
- Constantly update the Top Management on the status of resumption and recovery.
- Liaise for obtaining status on damage assessment and recovery progress from the concerned teams.
- Track incidents as applicable for their root cause analysis and to update log relating to lessons learned
- Facilitate the efforts of BCM departments representatives / Champions for the respective department

Internal sectors / Departments representatives / Champions

- Responsible for maintaining documents and update details periodically pertaining to their department as and when required or directed by BCM Manager, e.g., changes to the procedural flow impacting business, personnel roles and responsibilities etc.
- Responsible for keeping the head of BCM updated on the status of BCM Program pertaining to their department.

- Responsible for all follow up of activities related to BCM Program, reports like (Business Impact Analysis , Risk Assessment , Recovery Strategies, Exercise results) and maintain them as per respective department.
- Responsible for ensuring that vendors maintain BCM requirements for their outsourced activities.
- Liaise with all concerned within their department to conduct BCM exercise as per the schedule and maintains records of such exercise.
- Responsible for updating the BCM head and other dependent departments of changes made within their department.
- Responsible for tracking the incidents pertaining to their department for their root cause analysis and updating data base relating to lessons learned.
- Responsible for implementation of Preventive Action and Corrective Action plans and updates BCM Manager / BCM team.

Relevant interested parties

- Role of interested parties will based on the organization prioritized activities.
- Relevant interested parties. Roles and responsibilities should be communicated within the organization (if applicable).

5.2.7. Developing and implementing a governance framework is on the important success factors for BCM Program, there is no “one size fits all” governance framework. According to the size, nature, of an organization should establish its governance framework. Components of a governance framework are but not limited to:

- Reporting structure for effective implementation
- Defined roles and responsibilities
- Clear project management methodology
- BCM Program implementation plan

A-6. Business Continuity Capability

Each United Arab Emirates organization should assume the responsibility of defining and documenting its “fit-for-purpose” business continuity capability that ensures performance of prioritized activities and services during emergencies, crisis and disasters.

A-7. BCM Documentation and Records

7.1. Required Documents

7.1.1. The organization shall establish, implement and maintain records of BCM Program capability implementation procedures.
The purpose of BCM documentation and records as illustrated in figure 2.

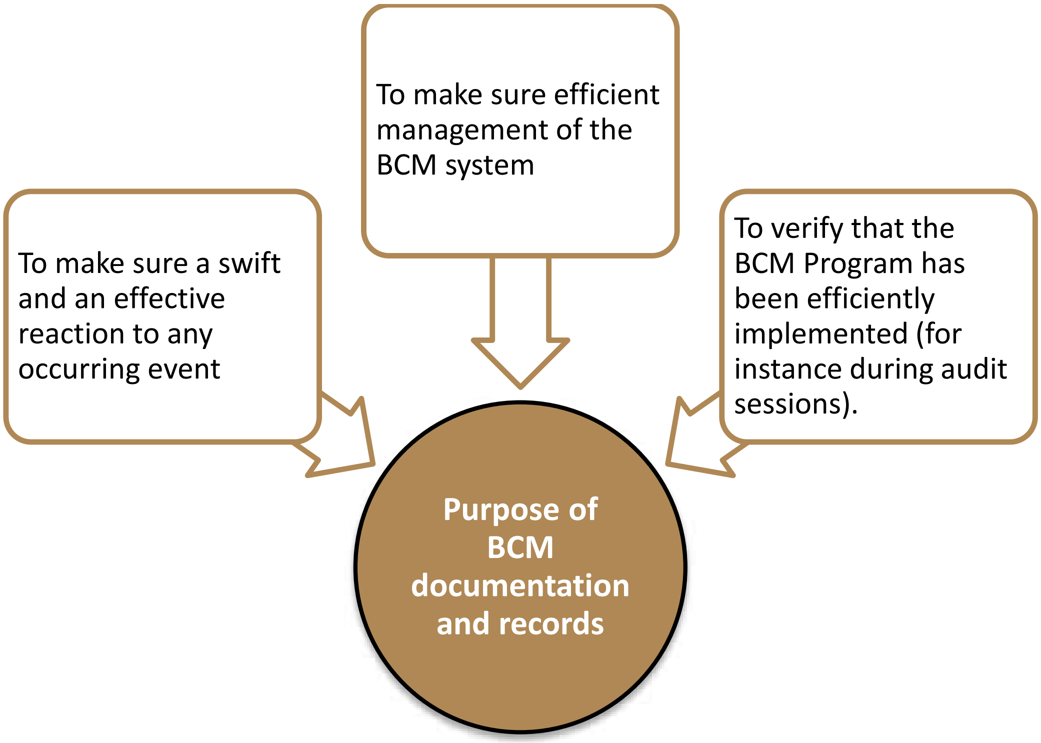

To make sure efficient management of the BCM system
To make sure a swift and an effective reaction to any occurring event
To verify that the BCM Program has been efficiently implemented (for instance during audit sessions).
Purpose of BCM documentation and records

Figure 2 Purpose of BCM documentation and record

7.1.2 Organization should maintain a documentary record of BCM Program implementation. Organization's BCM Programs documents should at least contain, and not be exhaustive to, the following:

a. Context of Organization
b. Objectives and Policy of BCM
c. Roles and Responsibilities
d. External and internal issues and interested parties
e. Competency of personnel
f. Business Impact Analysis (BIA)
g. Business Impact Analysis Methodology
h. Business Impact Analysis Report
i. Risk Assessment (RA)
j. Risk Assessment Methodology
k. Risk Assessment Report
l. Business Continuity Strategies
m. Incident Response plan (IRP)
n. Business Continuity Plan (BCP)
o. Media Response Plan (MRP)
p. Awareness and Training records
q. Test and Exercises record
r. Internal Audit record
s. Management Review record
t. Corrections and corrective actions
u. Regulatory requirements

7.2. Controlling BCM documentation and record

7.2.1 The following key points can be considered when developing and managing the BCM documentation and records:

a. BCM documentation should be prepared in an understandable way and should focus on providing and maintaining the effectiveness of its preparedness and response to business continuity.

b. The intensity of the BCM Program may vary from organization to organization normally on the basis of the organization's size and structure, work, nature, the extent of the services provided and the employees' skills in handling emergencies, occurring crisis and the management of Business Continuity.
c. BCM documentations should be effective enough to provide comprehensive support in generating operational and auditing/reviewing the details.
d. Frequent reviews should be conducted. If any amendment, addition on or cancellation is made to the documents, they should be reapproved by the Top Management.
e. BCM documents should be easy to retrieve. Copies of the BC Plans and all other important documents should be available on the primary and alternative locations (if any), as well as in all organizations branches.
f. If documentation or information from external sources is used, such sources should be mentioned.
g. A documentation control and distribution system should be created to ensure that all copies retained in all locations are properly updated.
h. Interpreting the relevant documents/information into more than one dialect by considering the organizations' structure, nature and language of its workforce, particularly those people who are chiefly engaged in execution of the business continuity plans and/or entrusted with particular responsibilities.
i. Ensuring the consistent compliance of the documents with the NCEMA Standard specifications (AE/SCNS/NCEMA 7000:2015).

A-8. Business Continuity Managements Program Operations

Developing a BCM Program

The BCM Program is an on-going process that must be managed effectively and efficiently. Proactive planning is required to develop a BCM Program, so as to respond to unexpected and unanticipated incidents. BCM Program helps organizations to identify, classify, understand and prioritize the business continuity risks, and develop plans so that the risks can be mitigated and disruptive events can be responded in a befitting manner.

Figure 3: highlights all the key components to consider when developing a BCM Program

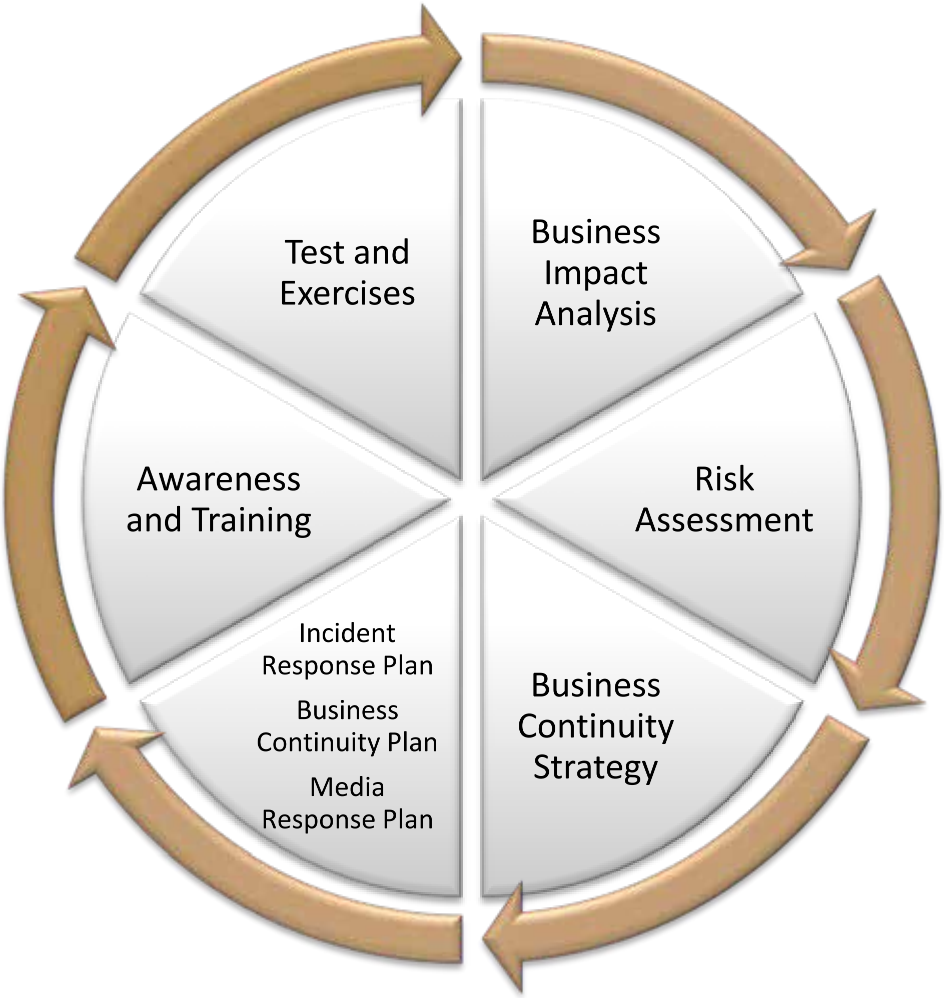


Figure 3 Components of BCM Program operations

Additional groups may be created to facilitate the development of the BCM Program. These comprise of:

- **BCM Steering Committee** – A Top Management group consisting of executives, officers or section heads, whose responsibility is to provide advice, guidance and management supervision.

- **Incident Management Team** – A team involved in incident response, whose responsibility is to resolve coordination issues and provide assistance in the management of the incident.

All staff who has been assigned to positions and duties or roles and responsibilities in the BCM Program should be equipped with awareness, education, and training so that they can accomplish their responsibilities in maintaining and operating the BCM Program of the organization. Confirmation of the effectiveness of the BC Capability of the organization can be provided through audited reports and post exercise reports

Outcomes of a BCM Program:

Outcomes of an effective BCM Program may include the following:

- Staffs are trained to respond effectively to a disruption
- Enables incident management capability of the organization
- Regulations from government authorities and emergencies are properly developed, understood and documented
- Compliance of the organization with its legal and regulatory is maintained
- Interested parties' requirements are well understood
- The organization understands its prioritized activities.
- Protection of the organization's reputation
- Adequate communication and support to staff in the event of a disruption.

8.1. Business Impact Analysis

Introduction

The Business Impact Analysis (BIA) is the process for analyzing business activities and the impacts of disruptive incidents that may happen over time. It provides information from which relevant business continuity strategies for continuity are determined.

The purpose of BIA is to identify and prioritize the activities which contribute to the identified process or processes that deliver the most urgent products and services, and to determine the resources required for the continuity and recovery of these activities

Goals of BIA

- To determine the prioritized activities and their time frames for resuming
- To assess and analyze the requirements of prioritized activities for their recovery and continuity
- To assess and analyze the impacts of not performing the prioritized activity
- To evaluate the time span after the occurrence of an incident in which an activity or product should be restored or resources and assets should be regained.
- To evaluate the maximum interruption /downtime the organization can tolerate.

Techniques to collect BIA

Depending on the nature, size, and the complexity of the organization, collecting BIA data techniques may vary from one organization to another.

One-on-one interviews

This approach enables an organization to have an active interaction with the staff, to investigate, and to formulate questioning to obtain the required information.

Management / supervisor workshops

Data collection workshops can prove to be an effective and efficient mode of collecting required data. Determine the suitable/appropriate level of participating persons. Identify workshop completion criteria to ensure that the facilitator and participants have clear idea about what is expected out of them, what are the required outcomes, and how the workshop will come to a conclusion.

Questionnaire

The most common method utilized for data collection is the questionnaire. BIA questionnaires must be designed with utmost care to ensure that the right questions are asked and they are easily understood in its real context. After collecting the information through questionnaires, face to face interviews must be conducted to clarify doubts arising from any answer.

BIA Information analysis

In order to identify critical information and processes, as well as potential disaster impacts, the information gathered during BIA must be evaluated and analyzed thoroughly. The information gathered from BIA should include:

- Validation procedure should be carried out in order to ensure the information gathered from the BIA
- Detailed and comprehensive understanding of organization's prioritized activities and services
- Identification of activities that provide support to such prioritized activities provided.

- Assessing the potential impacts of a disruption on these activities. When assessing impacts, the following should be address:
- Adverse effects on staff or public well-being;
- Consequences of breaching legal or regulatory requirements;
- Impact on the reputation ;
- Financial Impact;
- Operational Impact
- Estimating how long it would take for the impacts to become unacceptable
- Identifying dependencies between activities; and identifying each activity's dependency on supporting resources, including suppliers and other relevant interested parties.
- The prioritized timeframe for resuming an activity may be referred to as Recovery Time Objective (RTO). The RTO may take into account dependencies of interrelated activities and the time within which the impacts of not resuming the activity would become acceptable.

Outcomes of BIA

BIA findings are properly documented in a formal report; a typical BIA report includes following:

- Project Overview
- Executive summary
- Scope
- Data collection and analysis methodology
- Summary of BIA findings
- Detailed BIA findings (by departments)
- Charts and graphs to illustrate potential impacts (e.g., financial, information, operational, reputational, regulatory)
- Recommendations
- Future Steps
- Appendices may include:
- BIA Impact Criteria
- BIA Attendees

Report presentation to Top Management

After the BIA outcomes have been documented and consolidated, the formal BIA report must be presented to the Top Management as per the approved mechanisms of the organization.

8.2. Risk Assessment

While BIA assists in identifying some of the BC risks, a detailed and a comprehensive assessment about threat and vulnerability is still required for the identification of a wide range of risks and the likelihood of their occurrence. Risk Assessment is the process in which risks is identified, analyzed and evaluated.

Purpose of Risk Assessment

- Risk Assessment provides a mechanism for the identification of the risks that represent opportunities as well as the risks that represent potential pitfalls.
- It enables the organizations to have a clear idea of variables to which they may be exposed, whether internal or external, retrospective or forward-looking

Risk Assessment Process:

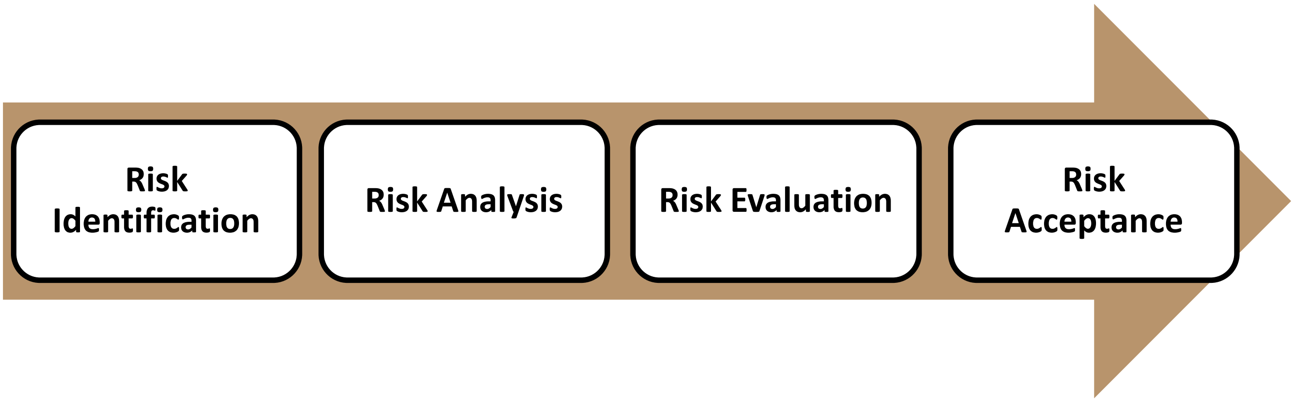


Figure 4 Risk Assessment Process

1. Risk Identification

The business continuity risk identification is based on the results of the business impact analysis. This analysis specifies the business services carried out by BCM Team or Section, and specifies their importance in terms of prioritized activates. For these services, the following sources of risk shall be considered:

- Unavailability of staff;
- Destructive loss of all or part of a building;
- Major physical utilities (power, water, etc.);
- Loss of ICT functions (data center, servers, etc.);
- Unavailability of information;
- National / international crisis or disaster;
- Financial shortcomings;
- Unavailability of transportation;
- Any issues or problems with business partners and/or suppliers.

Interviews with relevant functional managers, employees and stakeholders shall be used to identify the business continuity risks and the questionnaire in could be used. The identified risks shall address disruption to the organization prioritized activities related to processes, systems, information, people, assets, outsource partners, and other resources that support these business processes.

2. Risk Analysis

Risk Analysis Scales

All risks that have been identified need to be analyzed to assess their severity to ensure that the most important risks are treated first. All risks that have been identified are a compound of

Impact – how big is the impact of the risk occurring to organization's business and to the objectives?

Likelihood/Probability – how likely are the identified risks to occur?

The generic and the discipline-specific risk analyses that needs to take place are using the same scales, to ensure that the different risks can be compared and the results are consistent. Table 1 below illustrates a**n example** to the scales used for this risk analysis are:

Impact Scale:

Impact Scale				
Very High	**High**	**Medium**	**Low**	**Very Low**
5	4	3	2	1
The impact of this risk is very high, its occurrence would be extremely negative for organization, up to a total disaster	The impact of this risk is high, there are major disturbance or disruptions coming from this risk	The impact of this risk is medium, its effect has some negative effect, but the overall damage is limited	The impact of this risk occurring is low, there is minor effect on the organization	The impact of this risk occurring is very low, there is no or negligible impact on the organization

Table 1 Example of Impact Scale

The following table (2) shows **an example** of samples of impacts related to the various parts to support the identification of the right impact level:

Impact Level		Possible Impacts
Very High	**5**	• extensive long term business interruption, possibly indefinitely • failure of organization to meet its objectives • extensive effect on stakeholders for several months • huge financial loss greater than AED 5M
High	**4**	• major business disruption longer than identified RTOs for significant business operations • major project disruption • major effect on stakeholders for at least a month • major financial loss between AED 500,000 – AED 4,9M
Medium	**3**	• business disruption partly longer than the identified RTO (but quick resumption) • considerable project disruption • noticeable damage to stakeholders for several weeks • considerable financial loss between AED 250,000 – AED 499,999
Low	**2**	• minor disruption to business operations • minor project disruption • minor damage to stakeholders for a limited time period • minor financial loss less in the range AED 10,000 – AED 249,999
Very Low	**1**	• no or negligible disruption to business operations • no or negligible project disruption • no or negligible damage to stakeholders • very low financial loss less than AED 9,999

Table 2 Example of Impact Analysis

Moreover, further categories to risks may be added that suits the needs of the organization, Table (3) shows examples of risk categorization and related risks:

Risk Category	Relative Risks
Operations	Process Delay
	Absence of key staff
	Procedural Flaws
	Process Non Compliance
	Supply Chain disruption
PEOPLE	Mass absenteeism
	Disgruntled Employee
	Thefts, Frauds and Employee Infidelity
	Sabotage by employee
Premises	Building Collapse
	Flood (burst pipes)
	Bomb Explosion / Threat
	Power Outage
Information	Confidentiality of Data
	Data corruption
	Data security breaches
	Security of Data
Technology	Confidentiality of Electronic Data
	Security of Electronic Data
	Network Link failure / Outage
	Cyber Attack
	Configuration changes
	Obsolete
	Cabling failure, destructions
	Software bugs
Environmental	Earthquake
	Epidemics
	Unsustainable Weather
	Flood

Man-Made	Terrorism
	Political Protests
	Worker Strikes

Table 3 Examples of Risk Categorization

Likelihood Scale:

The second part of the risk analysis is the determination of the risk likelihood. For the risk assessment methodology, we might use a quantitative approach, as the information available in many cases is not sufficient to allow an analysis using a qualitative scale. The likelihood of a risk is distinguished using the table below, and the following considerations can help to identify an appropriate likelihood for a risk in question:

- If objective information, such as records of past events, are available they should be used
- Without objective information, interviews with stakeholders and employees can be used to get a first impression
- Information from other UAE governments or other organizations can also help to assess the likelihood

Another important part of the likelihood estimation is the consideration of existing controls to manage the risk – if controls of any kind have been implemented, they will help to protect against the risk and will make its occurrence less likely. Controls can vary depending on the discipline-specific risks considered, but it is important to take them into account.

In the same way, controls not in place can actually increase the likelihood of the identified risks. Any control that is incompletely implemented or not properly documented will make the organization vulnerable, and therefore increase the risk likelihood.

Based on all of the above considerations, table (4) below is **an example** of the likelihood of each risk might be estimated using this scale:

Likelihood Scale				
Very Unlikely	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
1	2	3	4	5
Less than 1 in 5 years	Less than 1 per year	Once or twice per year	Between 3 and 5 per year	At least 5 per year
Extremely unlikely events, not expected to happen	Unlikely, but there's a slight possibility it may occur at some time	The event might occur at some time, e.g. as there is a history of casual occurrence at the organization or similar organizations	There is a strong possibility the event will occur, e.g. as there is a history of frequent occurrence at the organization or similar organizations	Very likely! The event is expected to occur in most circumstances, e.g. as there is a history of regular occurrence at the organization or similar organizations

Table 4 Example of Likelihood Scale

Further detailed likelihood scales can be used to emphasize on the probabilities and quantified prediction of risk occurrence.

3. Risk Evaluation:

The results of the risk analysis (also defined as Risk Value) shall be compared with predefined risk criteria to determine whether a risk is acceptable or needs risk treatment. Basis of the comparison is the risk calculation and the level of acceptable risk. This risk assessment methodology uses the following table to assess the overall risk criticality:

	Risk Matrix					
Impact	Very High	🟨	🟧	🟧	🟥	🟥
	High	🟩	🟨	🟧	🟥	🟥
	Medium	🟩	🟨	🟧	🟧	🟧
	Low	⬜	🟩	🟨	🟨	🟧
	Very Low	⬜	⬜	🟩	🟩	🟨
		Very Unlikely	Unlikely	Possible	Likely	Almost Certain
		Likelihood				

Table 5 Example Risk Matrix

Risk Value:

Quantifying risk value once impact and likelihood has been calculated as shown in table (6) will help interpret identified risks based on the risk interpretation table (7).

Risk Value				
Very Low	**Low**	**Medium**	**High**	**Very High**
1-2	3-4	5-8	9-15	16-25

Table 6 Example Risk Value

Interpretation of the Risk Levels:

Risk Value				
Very Low	**Low**	**Medium**	**High**	**Very High**
1	2	3	4	5
No action required	No action required	Risk of this level can or cannot be treated, they need to be considered on a case by case basis	Risks of that level need to be treated to manage the situation	These risks have a very high or catastrophic impact on the organization

Table 7 Example of Interpretation of Risk Levels

4. Risk Acceptance Criteria

In accordance with risk ratings defined above in table (7), only very low and low risks can be readily accepted, and risks of a medium level need to be investigated on a case-by-case basis – the decisions taken need to be explained. Risks of high and very high level should always be considered for risk treatment, but can be accepted if one or more of the following criteria apply:

- The cost of risk treatment outweighs the impact of the risk occurring;
- The actions for risk treatment are not practical within the organization business, work environment or culture;
- There are no legal implications when this risk is accepted;
- There are only tolerable impacts on organization's business objectives.

Record Findings

Document the findings and prepare the proposed solutions in a report submitted to Top Management.

Review and Monitor

Changes are continuously happening in the organization therefore all BCM related documents should be reviewed at periodic intervals so that they remain up to date.

Risk Assessment outcomes

Risk Assessment outcomes should include the following:

- Risks that could result in the disruption or suspension of the organizations prioritized activities, classified by level of impact.
- Single points of failure (SPoF) associated with such as physical risks or resources.
- Actions required to reduce the risk of disruption or suspension of the organization's prioritized activities.

8.3. Business Continuity (BC) Strategies

After the BIA has been completed, the next step is to form BC Strategies. The organization should identify recovery solutions for key dependencies and potential interim business processes. These will be based on the findings from BIA and the RA process and should be appropriate for the organization. The organization should also evaluate the BCM competency of suppliers and the least possible requirement for the continuation of the prioritized activities.

Identify the appropriate measures for the control of the risks. Identify treatments that can ensure the achievement of the business continuity objectives and are according to the Risk Appetite of the organization.

Once a risk has been identified, a 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 should be completed;

- Resources required to complete the task; and
- Name of the person who approves task completion

8.3.1. Determination and choice of BC strategy should be done on the basis of outputs from the analysis of BIA and RA. The organization must define appropriate strategy options for:

- the protection of prioritized activities;
- reducing, and managing the impacts;
- recovery and resuming of prioritized activities.

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. The following Business Continuity strategy should be taken into account:

- **Back-up Sites (Split/ Dual site operations)**
  This strategy involves performance of prioritized 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 organizations, 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 organizations prioritized 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 predefined alternative site after an emergency, crisis or disaster strikes. The alternative site may be a facility provided by a third-party, 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 prioritized 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 when necessary.

- **Outsourcing**

  Another strategy that can be employed to reduce risk is to outsource or contract performance of prioritized activities to a third-party depending on the nature of the organization. To that end, memorandum of understanding (MOU), Service Level Agreements (SLA) or other legal formats should 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 organization 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 should 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 organization’s needs. Outsourcing or contracting the performance of prioritized activities to third parties does transfer the risk, but does not discharge the organization 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 organization may consider warehousing a temporary supply of essential materials for continuity of its prioritized 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, is purchased to cover direct costs related to loss of revenue as a result of disruption of prioritized 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 prioritized 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 prioritized 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 organization’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 organization 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 organization.

8.3.2. All the resources required to determine the selected BC strategies should be documented and approved by the Top Management. Following are the examples of resources that can be included however should not be limited to:

- People (competence)
- Buildings and facilities

    - Information and communication infrastructure
    - Budget allocation
    - Suppliers and service providers
    - Resources
    - Technology

- **People**

  People are the most critical resources of an organization. It is important for an organization to identify suitable measures for maintaining and widening the availability of fundamental skills and knowledge in case a disruptive incident occurs that results in the loss of availability of staff. Techniques for the protection or development of employee skills may consist of:

    - Cross-skill training of staff
    - Specialists that can temporary work
    - Skilled staff at one or more locations in order to reduce the impact of an incident

- **Building and Facilities**

  Size, nature and the geographical area of an organization must be considered when identifying and considering alternate location. Some factors that must be considered while determining alternate location are:

    - Location Area: If an organization is located in a risky area which is susceptible to disruptive incidents, then alternate location must be at a large distance from the primary location
    - Accessibility: The alternate location must be easily accessible for staff to travel. All staff must be well-versed with the alternate location map.
    - Resources: The organization must make it very clear whether the resources in the alternate location are shared or possessed only by the organization. In case the resources are shared, a plan must be documented and signed to ensure that all resources will be available when required.

Alternate location can be made available by other organizations or third parties suppliers.

- **Communication and Media**
  Information essential for the operation of organization should be secure and recoverable in accordance with the time. The organization should draft in advance the message templates, scripts, and statements it may need to communicate with stakeholder groups, employees family's regarding the disruptive incident. The organization should designate key and substitute official spokespersons especially those are trained to interact with media and communicating with internal and external stakeholders.

- **Budget Allocation**
  The organization shall define possibilities to ensure the finance is available during and after a disruptive incident. This may consist of making sure there is budget available for:
  - Transportation
  - Any emergency purchases for example providing food and accommodation
  - Heavy purchases such as buying or renting specialist equipment/machinery or buildings

- **Suppliers and service providers**
  It is the responsibility of the organization to identify products, services or activities provided by the third party in the BIA process. Therefore, an organization should make sure that its suppliers and service providers have effective continuity arrangements in place (e.g. Service Level Agreements). In order to gain that surety, organization can view the supplier's:
  - Business Continuity Policy
  - Business Continuity Plans
  - When and where the plans last updated
  - Exercise and maintenance programs.

- **Resources**

  During the BIA, the organization should identify the resources that support the prioritized activities and maintain an inventory of them. Determine the resources that are essential to implement the business continuity strategies. Not all resources can be stored, such as specialized equipment's /resources or heavy machinery maybe too expensive to store or may get damaged if not used for long. If a prioritized activity is heavily dependent upon specialist equipment/ resource or heavy machinery, the organization should identify the suppliers that provide those equipment's/ resources. Following points can be considered to maintain the supply of such resources:

  - Considering more than one supplier
  - Signing Service Level Agreements with suppliers according to the RTO of the prioritized activity
  - Encouraging suppliers to have business continuity.

Similarly alternate solutions for such resources should also be considered. The organization can consider storing the resources at alternate location (if available), warehouse or shipping sites.

- **Information and Communication Technology**

  Information and communication technology options will be subject to the size and complexity of the technology employed and its interdependencies with the prioritized activities. Some organizations hold great amount of dependency on technology and their activities cannot be executed without technology systems and they must be restored before activities can be restarted. Where it is possible and practical, the organization may be required to implement manual operations.

8.3.3. Risk treatment encompasses identification of the range of options for handling risk, evaluating those options, formulating risk treatment plans and executing them.

The options existing for the management of risks consist of:

- Accepting the risk: if, after controls are introduced, the remaining risk is considered tolerable to the organization “according to its risk appetite”, the risk can be accepted.
- Reducing the possibility of the risk taking place: by means of preventive maintenance, audit & compliance programs, supervision, contract conditions, policies & procedures, testing, investment & portfolio management, staff training, technical controls and quality assurance programs etc.
- Transferring the risk: this encompasses another party bearing or sharing some part of the risk using contracts, insurance, outsourcing, joint ventures or partnerships etc.
- Avoiding the risk: take a decision not to carry on the activity which can generate the risk, where this is feasible.

8.3.4. The organization should make sure that the business continuity of suppliers is assessed. Techniques of assessing suppliers as follows:

- Include the descriptions of requirements in tenders and contracts
- Perform periodic evaluation audits of the suppliers business continuity plan
- document service level agreements or memorandum of understanding in legal formats

8.4. Incident Response Plan

The organization should introduce procedures and a management structure that will enable preparation for and respond effectively to disruptive incidents.

Goals of an Incident Response Plan

- Safety of personnel.
- Identification of the impact thresholds that rationalize the introduction of formal response;
- Introduce an appropriate response to a disruptive incident;
- Ensure the availability of the resources to support the processes and procedures required to manage a disruptive incident and to curtail the impacts; and
- Communicate the processes and procedures to the interested parties, including responding authorities
- Evaluation of the nature and degree of a disruptive incident or the potential impact;
- Introduce appropriate measures for the welfare to affected individuals;

Key steps on designing Incident Response Plan

The key steps in designing the incident response plan are:

- Conducting a comprehensive study and understand the nature and the existing incident management of the organization
- Creating a team and assigning roles and responsibilities
- Developing an Incident Response Plan
- Attaining Top Managements approval
- Documenting the approved Incident Response Plan.

Content

The Incident Response Plan should include the following:

- The criteria of response plan activation;
- The person who has authority to activate the plan;
- The Incident Management Team;
- Developing evacuation plan.
- Establishing alternative sites for:
  1. The restoration of IT or critical infrastructure elements
  2. Temporary use of any element in performing prioritized activities

- Record of the internal and external stakeholders that may need to be contacted in the first few hours of an emergency, crisis and disaster;
- The means of communication with stakeholders, local authorities, and media and what is required to be communicated to them;
- Pre-scripted message templates for communications;
- Personnel responsible for coordinating with first responders; and
- Process and criterion used to assess damage and impact.

8.5. Business Continuity Plan (BCP)

The effectiveness of an organization's Business Continuity capability is dependent on its ability to plan for activity at each stage of the disruption. The organization should effectively respond to the incident to ensure the health and safety of its personnel, those responding to the incident and those impacted by it.

The key steps in developing a BC plan include

- Appoint an owner/ sponsor for the BC plan
- Make a decision about the structure, format components and contents
- Precisely define the objectives and scope
- Assign the roles and responsibilities of the response team
- Collect the information necessary to populate the plan
- Prepare a draft of the plan including all the necessary details
- Circulate the draft plan to all concerned for discussion, input and review
- Collect the feedback from discussion
- Incorporate the necessary amendments in the plan and check its quality
- Reach a decision and authenticate the plan. For example, by rehearsing it in an exercise
- Come to an agreement on a program of ongoing exercising and maintenance of the plan to make sure that it remains up-to-date and the response teams are up to date as well.

The stakeholders in an organization Business Continuity capability should include people with special needs. These special needs should be taken into account when planning.

8.5.1. The organization should develop documented procedures that will maintain the continuity of its prioritized activities at predefined levels during a disruptive incident. The organization should make sure that identified risks are addressed for the continuation of the prioritized activities.

8.5.2. Each plan should:

- Have a defined purpose and scope.
- Be communicated to all personnel that needs to be aware of it, and to personnel with specific roles and responsibilities for review and update.
- Be consistent with the BCM strategy and incident response plan, capabilities and requirements of interested parties.
- Be accessible to and understood

8.5.3. All Plans should contain

Within the business continuity plans, the following must be clearly identifiable:

- **Purpose:** This part precisely and clearly defines what the plan sets out to do
- **Scope:** Precisely defines the scope of the plan
- **Assumptions:** This part defines the assumptions on which the plan is based
- **Invocations Instructions:** Defines the guidelines and criteria regarding who has the final authority to invoke these procedures and under what circumstances these can be invoked – it may follow defined escalation stages.
- **Standing down Procedure:** Clearly defines the procedure for standing teams down once the incident is over; and assess damage post incident.

- **Team Structure:** This part summarizes who will perform the role of leader and supporting functions. It defines the roles, responsibilities and authorities of people and teams who have to execute the business continuity plan
- **Resources:** This part provides the details about the resources essential for business continuity
- **Incident management**: Management of the immediate consequences of a disruptive incident paying attention to the welfare issues of affected individuals (including team members), options for reacting to the disruption and prevention or further loss or unavailability of prioritized activities;
- **Communications:** provides the details about addressing how and under what conditions the organization will communicate key interested parties and emergency contacts to the employees as well as their relatives,; also the details of the media response of the organization following an incident, including its communication strategy, preferred interface with the media, guidelines or templates for drafting media statements as well as identification of appropriate spokespeople.
- **Contact Details:** Contact details of members of team and others with their roles and responsibilities
- **Action List:** identify the actions and tasks that are required to be accomplished, particularly regarding how the organization will continue or recover its prioritized activities within scheduled timeframes;

8.6. Media Response plan

It is important to have appropriate procedures to manage communication with external parties.

External means of communications include:

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

The procedure to manage communication should encompass:

- Details regarding how and under what circumstances the organization will establish communication with employees as well as their relatives regarding emergency contacts, media and other interested parties';
- Details regarding the media response of an organization after an incident.

The organization's Media Response Plan should provide instructions and guidance required to Top Management, Executives, and Staff and Public Relations personnel on how to communicate approved messages with internal and external stakeholders before, during and after a disruptive event.

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 should 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 Media Response 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 organization’s internal website; and
- Short Messages Service (SMS).

The organization’s communication capabilities should be tested as part of the regular testing and exercising of the BCM Program.

8.7. Awareness and training

Awareness and training ensure the organizations personnel and staffs are aware of the importance of business continuity, understand their roles, gain knowledge and ability to execute its plans. The organization should develop and implement an awareness and training program that supports the BCM objectives of an organization. Training can be provided through internal or external sessions and working with professionals assisting in BCM Program development and implementation. The awareness and training strategy varies from one organization to another, depending on each organizations strategy and policy.

8.7.1. Staff Awareness

The organization’s level of awareness differs between employees according to their roles and responsibilities.

The Staff Awareness program should:

- Include BCM policy and objectives
- Establish a methodology for evaluating its effectiveness;
- Spread BC capability and awareness;
- Ensure continual improvement of BCM Program; and

- Ensure personnel are aware of their roles and responsibilities in BCM Program.

Items that should be available to boost awareness among specific teams in the organization’s BCM Program include:

- A measurable and assessable system should be developed to ensure the effectiveness of the awareness program. This can be achieved by obtaining periodic data or holding interviews with staff to determine the extent of their understanding and awareness with respect to the BCM Program.
- Awareness can be spread within the organization various 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 organization’s work environment culture.
- Continuous improvement of the program should be conducted by attending specialized scientific conferences and seminars whether tailored to the organization’s emergency staff or Top Management to support their understanding of the importance of these programs.
- Staff playing roles in the BCM Program should be encouraged through financial and moral incentives as these roles and responsibilities are usually an addition to their original roles and responsibilities. The efforts should be properly appreciated, especially after holding annual exercises or real incidents.

8.7.2. BCM awareness should also be spread among interested parties. Interested parties should have knowledge of their roles and responsibilities in case of disruptive incidents, in order to accomplish BCM requirements within defined time frames.

8.7.3. Training

All personnel should receive proper training in order to perform their BC roles. They should also receive instructions on the key components of the organizations BCM Program, in addition to the Incident response and business continuity plans that directly affect them.

Response and recovery teams should receive education and training on their responsibilities and duties, including how to interact with first responders. Teams should provide 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 that can be included in the training program are:

- Overview of Business Continuity Management
- Program Development and 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

8.8. Test and Exercise

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

The organization should design test scenarios that focus primarily on training on highest risk business activities, as identified in its Risk Assessment and Business Impact Analysis. Also, the organization 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 organization.

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

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

A test and exercise report should be completed immediately after each exercise. This report should contain (but not limited to):

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

8.8.1. Tests

Tests should be conducted for assessing the readiness, usability and appropriateness of the tools, technology, facilities, and infrastructure required for the implementation of the BC plans of the organization. Post-Test reports should be developed, revised and remedial measures taken, when required.

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

- Cooperate with Top Management to identify the organization’s capability areas that would benefit from the increased awareness that a test would provide.
- Identify the BC plan elements, resources and procedures that will be tested, e.g. resource allocation, emergency contact and communication, or relocation to an alternative worksite.
- Identify suitable tests for each element, resource or procedure.
- Identify the personnel or groups involved in the test.
- If tests 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 organizations prioritized activities.
- The frequency of tests dependent upon the nature, size and complexity of the organization.

8.8.2. Exercises

Exercising makes sure that the teams and personnel are effectively trained for the usage and operation of the tools, equipment and other resources required to accomplish their duties.

BCM capability cannot be considered dependable until it has been exercised. A planned Exercise Program is essential to make sure that all aspects of the plans and personnel have been implemented over a period of time, evading disruption to the entire business.

Exercises should be developed and conducted to:

- Apparent weaknesses and strengthen the plans, operating procedures, and the planning assumptions;

- Ensure the organization’s BC Strategies are accurate and BC plans will enable the organization to meet the recovery objectives defined in the BIA;
- Ensure cohesion and integration of plans in terms of interoperability;
- Test and validate recently changed procedures;
- Familiarize BC and Incident Management Teams with their processes and procedures;
- Ensure personnel and teams implementing the plans and procedures have the requisite skills, authority and experience to implement such plans.
- Enhance coordination among response agencies and support organizations;
- Validate the training process and procedures for evacuation, response, incident management, communication, and regaining of business continuity; and
- Increase the organization’s awareness and understanding of the threats which can impact and disrupt its prioritized activities.
- Validate that all the contacts and information necessary to attain recovery resources required by the plan, have been accounted for.

The organization’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 list of exercises types are given in table (8):

Type of Exercise	Objectives of the exercise
Table Top	check the structure and elements of the plan
Walkthrough	thoroughly discuss the theory of the plan to check that it is usable
Simulation	use the plan to undertake theoretical response to an incident
Limited rehearsal	Confirm that a recovery procedure or the recovery of a piece of technology works
Live test	Confirm that full recovery of a complete activities of the organization

Table 8 Types of exercises

A-9. Business Continuity Program Review

The objective of BC Program review is the evaluation and the identification of the improvements of BC capability.

Review can be classified into three types:

- Annual Review
- Review of Suppliers and Service providers
- Compliance and internal Audit Review

Review and updates are obligatory when a change takes place in the organization whether in terms of services /works or when a change takes place within the Top Management.

9.1. Annual Review:

Frequently, at least annually, the organization must carry out a review of its:

- Policy and objectives
- BCM Program documentation

- Exercise reports
- Audit Reports
- Changes to the business and risks that can result in business disruption
- Review risk appetite
- Review business continuity strategy
- Approving response, incident response, business
- continuity plan(s) tailored to achieve the organization’s
- BCM objectives

This review is intended to make sure that all BC capability documents are effective and in line with the strategic objectives of the organization.

9.1.1. It is essential to establish a formal process for maintaining the BCM Program. The process of conducting annual review must be assigned to an individual or team, and must comprise of:

- Review what has changed since the last update;
- Analyze the impact of any changes;
- Identify any changes to other areas;
- Update the plans as and when required;
- Provide training, awareness and/or communications as required;
- If plans have been modified, ensure to distribute the new versions as soon as possible;
- Identify the date for undertaking the next planned maintenance, and schedule the maintenance.

9.1.2. Post any incident or crisis, there should be a log maintained, 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 organization’s BC objectives
- Assessment of organization’s effectiveness in meeting BCM recovery objectives
- Identification of required changes to improve its BC capability

9.1.3. Annual BCM Evaluation Report

After the annual review has been completed, organizations should produce an annual report on the BCM Program status.

- Summarize the organization’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 organization’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.

9.2. Review of Suppliers and Service providers

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

- Reviewing the supplier's BC status and ensuring it is acceptable to the organization. Integrating its Incident Management / Business Continuity 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.
- Where the organizations supplies products to customers and clients, its Incident Management and Business Continuity plans should be reviewed based on the business objectives of the customers and clients, so as to ensure the organization can meet their expectations and fulfill the terms of its contracts and agreements with them, in accordance with the organization's BIA. This capability should also be checked through the previously mentioned exercises.

9.3. Compliance and Internal Audit Review

The audit process must be carried out frequently as defined by the audit and governance policies of the organization. The objective of a BCM audit is to scrutinize the existing BCM Program of the organization; authenticate it against predefined standards and criteria and provide a structured audit report.

Audits should be conducted on a regular basis, as defined in the organization's audit and governance policies to ensure:

- Compliance with the standard;
- Consistency with BCM objectives and policy;
- Proper implementation, execution and sustainability; and
- Effective fulfillment of the organization's BCM capability objectives.

9.3.1. Annual Internal Audit

The organization should conduct a complete annual internal audit of its BCM Program. This audit should cover all requirements of the Standard. A formal BC Audit process should ensure the organization has an effective Business Continuity capability program.

The purpose of a BC audit is to:

- Ensure compliance with the organization's BC policies and procedures;
- Review the organization's BC solutions;
- Verify the organization's BC plans;
- Verify that appropriate exercise and maintenance activities are available;
- Highlight deficiencies and compliance gaps;
- Ensure the remedy of such gaps.

9.3.2. Internal Audit Program

The organization should develop an audit program that is based on its size, nature, of the organization, scope of the BCM Program and other related factors. The internal audit program may not address all the components of the BCM Program all at once. The audit can divided into small parts and can be conducted at periodic intervals however all organization activities that come under the scope of the BCM Program should be audited within the organizations audit time frame.

9.3.3. Internal Audit procedures

The organization should develop procedures to implement its Internal Audit Program.

To define audit scope:

- Determine the locations, departments, and activities to be audited.
- Define the audit approach:
- Identify the auditing activities that will be undertaken, e.g. questionnaires, one on one interviews, document reviews and/or solution review.

- Identify the audit activity timetable and due dates.
- Identify the audit evaluation criteria (standards).
- Determine audit requirements by specialists and experts, as a third party, to conduct audit process.

9.3.4. Internal Audit Report

To prepare the Internal Audit Report:

- 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.

The following should be reported to Top Management:

- An independent BC audit report should include but not be limited to:
    - Executive summary of the audit
    - Summary of key findings
    - Summary of the key report recommendations
    - Detailed current state and review results (Detailed Observations)
    - Risks
    - Detailed recommendations
    - List of staff interviewed
    - Documents provided for interview

A-10. Top 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.

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 organizations BC Policy, Risk Assessment, or BIA;
- Major changes to the organization, its business objectives, business processes, facilities and IT hardware and software infrastructure;
- Changes in assumptions in the organizations Risk Assessment and BIA;
- Changes in the organizations Risk Appetite;
- Changes in the threats faced by the organization, 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 organizations business sector or industry
- Revision of old requirements or addition of new regulatory and compliance requirements in the organizations sector or industry; and
- Latest events of disruption directly impacting the organization or similar organizations
- Where the disruption directly affects the organization itself, the management review should consider the reason of plan activation and success, etc.

10.1. Management review of BCM Program

Top management should review the organization BC Capability as per the planned intervals in order to ensure its continuing, adequacy and effectiveness.

The management review must encompass the scope of the BCM Program, although it is not obligatory to review all the elements simultaneously and the review process can last for a period of time. Review of the implementation and results of the BCM Program by the Top Management must be frequently planned and assessed. Although an on-going system review is desirable, however formal review must be structured and properly documented and planned on an appropriate basis.

10.2.Documentation of the management review

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

10.3.Points of input during management review

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.

10.4.Management Review outcome

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 organization'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 organization's BC Capability Certification.

A-11. BCM Program Continual Improvement

On a regular basis, at least annually, the organization is required to perform a review of its BCM Program including the BIA, Risk Assessment, BC Strategy, and BC Plans. This review is designed to ensure all BC capability documents are valid and consistent with the organization's strategic objectives.

This review should be formally conducted by the Internal Auditor or BC Manager. The review should result in a report to Top Management. Review and update are necessary when a change occurs in the organization whether in terms of services or works or when a change occurs within Top Management.

11.1.Non-Conformities

A comprehensive study 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.

11.2.Corrective Actions

Preventive and corrective actions should be compared to BCM objectives and policy to ensure continual conformity.

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.

Non-conformances and corrective actions that address them should be recognized and dealt from time to time. If non-conformity is identified, comprehensive study should be conducted in order to understand the cause of the non-conformity and a corrective action should be created immediately.

Right of use

All training and consulting service providers shall seek NCEMA's approval prior to use if the Business Continuity Management Standard – Specifications (AE/SCNS/NCEMA 7000:2015).

Contact NCEMA

For additional information and guidance, please contact NCEMA, Safety and Prevention Department, Business Continuity Section at:

Telephone	: +971 2 4177000
E-mail	: bcm@ncema.gov.ae
Website	: www.ncema.ae

NCEMAUAE