UNITED ARAB EMIRATES الإمارات العربية المتحدة

المجلس الأعلى للأمن الوطني

THE SUPREME COUNCIL FOR NATIONAL SECURITY

الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث

National Emergency Crisis and Disasters Management Authority

The National Standard For Business Continuity Management System

(Specifications)

AE/SCNS/NCEMA 7000:2021

الإمارات THE EMIRATES | IMPOSSIBLE IS POSSIBLE

Right of use

- All training providers shall seek NCEMA's consent before using this document.
- All intellectual property rights and copyrights are reserved to the National Emergency Crisis and Disaster Management Authority.
- Copyright and distribution are reserved to the National Emergency Crisis and Disaster Management Authority.
- The National Business Continuity Management System AE/SCNS/NCEMA 7000:2021 can be obtained from NCEMA website https://www.ncema.gov.ae.

Foreword by H.H. The National Security Advisor

The Supreme Council for National Security aims through its leadership, resources and human capital to achieve a model union and a secure country that has economic prosperity and community cohesion, and in order to achieve this vision, The Supreme Council for National Security has worked to reinforce the concept of emergency and crisis management by providing the latest systems and applying the highest global and local standards for business continuity, with effective stakeholders in the emergency and crisis management community from organizations in the government and private sectors through joint work and close cooperation.

In order to ensure the proactive capacity of the country, The National Emergency, Crisis and Disasters Management Authority (NCEMA) has issued the third version of The National Standard for Business Continuity Management System, which is an essential reference and one of the most important strategies of the country to achieve a robust and resilient infrastructure in all vital sectors. The National Emergency, Crisis and Disasters Management Authority has set its sights on the importance of building this capacity, and has harnessed its resources and expertise to prepare this document, which is an essential basis for the country's business continuity management system, with the participation of the concerned authorities in the country who have spared no effort in providing opinion and advice to bring the document to the required level and to be suitable for the business requirements of all entities

This document is developed for the concerned organizations in all sectors to comply with The National Standard For Business Continuity Management System by implementing the requirements of this standard, thereby enhancing the capacity of the UAE business community to cope with emergencies and crises, and this standard enables employees, through the training programs and applied models, to achieve comprehensive knowledge in business continuity management in accordance with the concept of vital functions in the organization.

Tahnoun bin Zayed Al Nahyan

The National Security Advisor

Preface

Under the guidance and direction of the UAE government's Supreme Council for National Security and in pursuit of a secure and stable nation, the National Emergency Crisis and Disaster Management Authority (NCEMA) has updated the second version of the Business Continuity Management Specifications (AE/SCNS/NCEMA 7000:2015).

The modifications and addition in this version include:

- Simplification of the language, structure and content of the standard to make it more understandable and increase the adoption.
- Addressing local requirements based on feedback from interested parties including goverment entities and other organizations that have implemented the standard.
- Aligning the specifications with the international requirements of business continuity management system, whilst retaining its unique identity.
- Differentiating clearly between the management system requirements (Clauses 3 to 7, 9 and 10) and BCMS operations requirements (Clause 8).
- Introducing guidance text to explain the purpose of each clause and using cross-referencing to clarify the requirements.

This document was drafted and technically reviewed by NCEMA, in collaboration with experts, professional bodies and strategic partners.

CONTENTS

CONTENTS

1 INTRODUCTION

1 INTRODUCTION

1.1 The standard

NCEMA has developed a business continuity management (BCMS) standard ('Standard') for organizations to implement and maintain an effective management system that provides the capability to continue operations during disruptions.

Implementation of the Standard will enable UAE government and private sector entities to:

- Protect against and reduce the likelihood or impact of disruptions.
- Prepare for, respond to, and recover from disruptions.
- Effective implementation across UAE government entities and their private-sector partners will also enhance national stability.

The Standard has been developed specifically for the UAE but would benefit any organization and is available in both Arabic and English. In the event of disparity between the two versions, the English version takes precedence.

The BCMS objectives of the UAE national and local governments of each emirate and the entities under their jurisdiction in both public and private sectors are as follows:

- Continuity of essential operations in both public and private sectors.
- Security of supply chains required for essential operations.
- Effective business continuity plans for resumption of activities needed for essential operations.

1.2 Scope of the standard

The requirements of this Standard are relevant to all organizations, or parts thereof, regardless of type, size and nature. The extent of the requirements' applicability will depend on the organization's operating environment and complexity.

1.3 Components of the standard

The Standard consists of three separate publications:

1. Specifications

   This document specifies the requirements for an effective management system for business continuity. Organizations can use this document to assess compliance through self-assessment or external audit to seek certification.

2. Guidelines

   To assist the resolution of issues of interpretation, the guidelines explain and clarify in more details the meaning and purpose of the requirements stated in the Specifications.

3. Toolkit

   The toolkit provides information and templates to support the implementation of the requirements stated in the Specifications and enable organizations to measure their performance.

1.4 Content of this document

This document specifies requirements for an organization to establish a management system for business continuity.

The requirements are consistent with those of the following ISO standards, which were used as references during its development:

- ISO 22301:2019 Security and resilience – Business Continuity Management Systems – Requirements
- ISO 31000: 2018(E) Risk Management – Guidelines.

Modal verbs are used in the Specifications as follows:

a) 'shall' indicates a requirement.

b) 'should' indicates a recommendation.

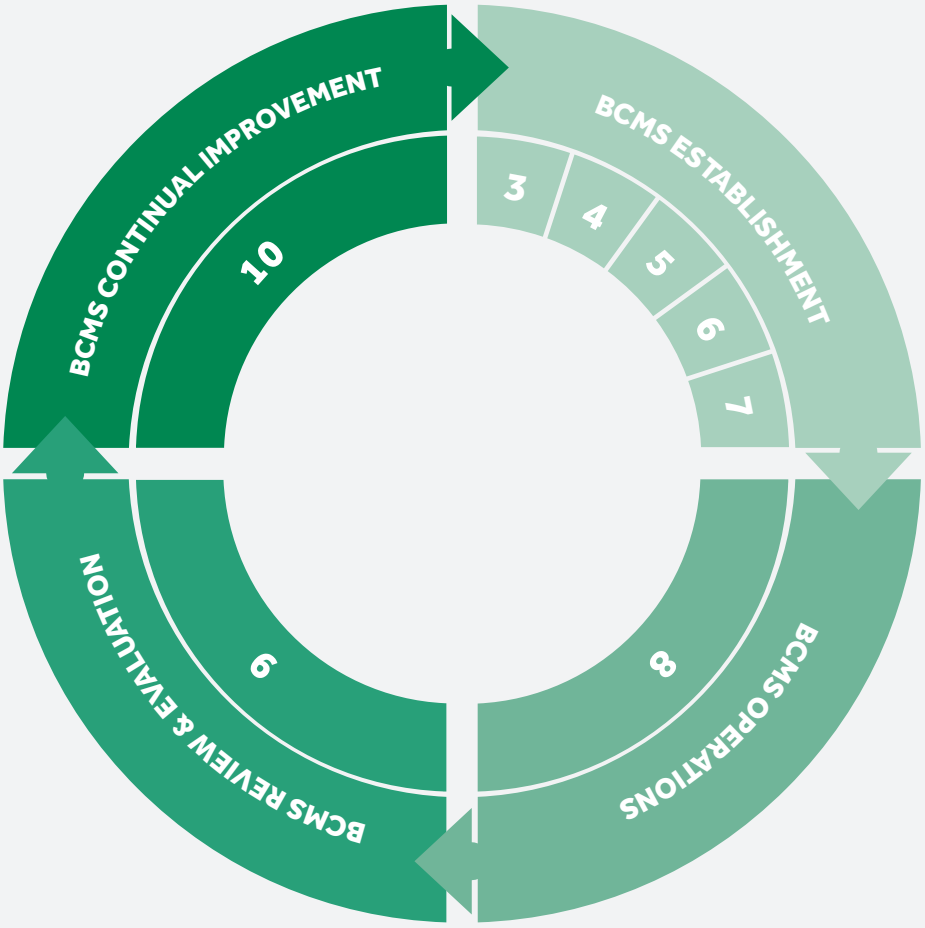
c) 'may' indicates a permission.

d) 'can' indicates a possibility or a capability

Many of the clauses in this document include guidance text. The purpose of this text is to explain and clarify the requirements of the clause in order to assist understanding. In all cases, conformance to requirements will only be achieved by fulfilling the requirements as stated.

1.5 Management system structure

Figure 1 provides an overview of this document and identifies the common elements of a management system (Clauses 3 to 7, 9 and 10) and BCMS operations (Clause 8), which is specific to this Standard.



3	Governance framework	7	Documented information
4	Context f the organization	8	BCMS operations
5	Policy, scope and objectives	9	Review and evaluation
6	Management system support	10	Continual improvement

Figure 1: Management system for business continuity (numbers refer to clauses in this document)

1.6 Applicability to UAE entities

The Standard is applicable to all UAE entities, and related bodies including organizations performing the functions of principal government institutions and community services. All organizations must endeavor to continue essential operations within a predefined minimum acceptable delivery levels of products and services.

Compliance with this specifications document will benefit organizations that aim to:

a. Establish and maintain business continuity.

b. Maintain an ability to continue essential operations at acceptable capacities.

c. Enhance their resilience to disruptions.

d. Assess their capability to meet their business continuity needs and obligations.

e. Contribute to the UAE's national security.

1.7 Federal and local implementation

The National Emergency, Crisis and Disaster Management Authority is the exporter and legislator of the national standard of the UAE's business continuity management system and is responsible for monitoring its implementation at the federal and local level.

The United Arab Emirates consists of authority levels at federal and local levels, and multiple government and private sectors. The following hierarchy demonstrates the authority level for federal and local entities:

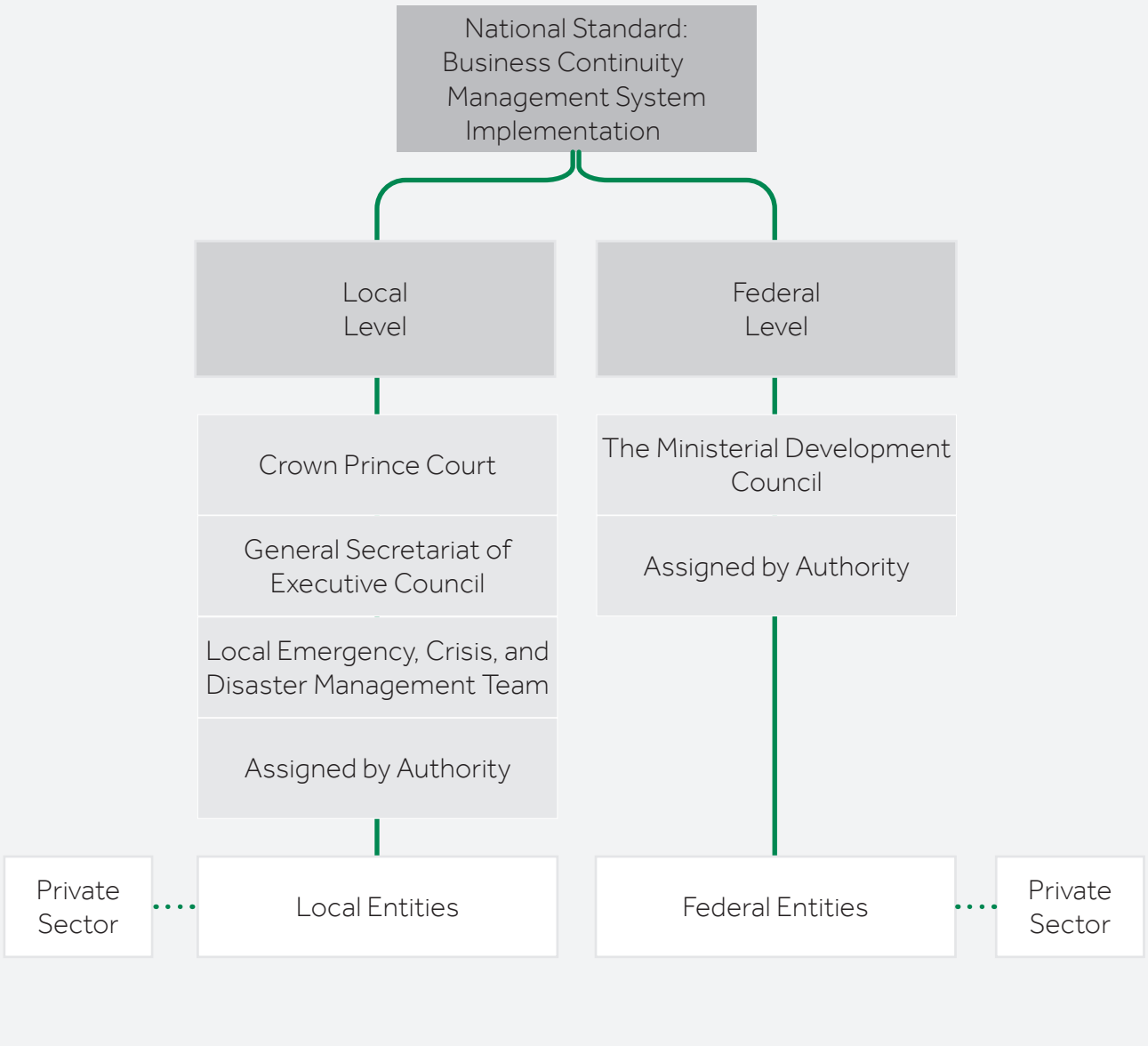


Figure 2: Federal and local implementation Hierarchy

1.8 Controls set by legislative bodies

Legislative, licensing and regulatory bodies will often establish further requirements in addition to those defined in the Standard to ensure community safety, security, and continuity of functions and activities required to promote national security. Where additional requirements are established, the organization shall comply with such requirements.

However, in case of discrepancy between the requirements of this Standard and the additional ones, such organization shall have recourse to the issuing authority of this standard for settlement.

2 DEFINITIONS

2 DEFINITIONS

2.1 Activity

Set of one or more tasks with a defined output.

2.2 Audit

Activities performed by an independent party to obtain objective evidence and determine objectively the extent to which requirements have been fulfilled.

2.3 Audit Criteria

Set of policies, procedures or requirements.

2.4 Audit Evidence

Records, statements of fact or other information, which are relevant to the audit criteria and verifiable.

2.5 Audit Findings

Results of the evaluation of the collected audit evidence against audit criteria.

2.6 Audit Scope

Extent and boundaries of an audit.

2.7 Business Continuity

Capability of an organization to resume delivery of products and services during a disruption within acceptable timeframes at acceptable capacity.

2.8 Business Continuity Management (BCM)

Implementation and maintenance of business continuity.

2.9 Business Continuity Objectives

Targets or goals, consistent with business continuity policy, that an organization sets itself to achieve.

2.10 Business Continuity Policy

Top management's intentions and direction in relation to business continuity.

2.11 Business Continuity Strategy

Plan of action to meet business continuity requirements.

2.12 Business Impact Analysis (BIA)

Analysis of impacts of disruption to determine resumption priorities.

2.13 Capacity

Quantity of output or level of performance (for example, 30% of normal output).

2.14 Competence

Ability to apply knowledge, skills and experience to achieve intended results.

2.15 Compliance

Fulfilment of the specifications requirements.

2.16 Conformity

Fulfilment of a requirement.

2.17 Context

Combination of internal and external issues that might influence an organization's achievement of its objectives.

2.18 Continual Improvement

Recurring activity to enhance performance.

2.19 Consequence

Result or effect, typically, unwelcome or unpleasant.

2.20 Corrective Action

Elimination of cause and prevention of reoccurrence of nonconformity.

2.21 Disruption

Incident that adversely effects an organization's normal course of operations.

2.22 Documented Information

Information required to be controlled and maintained by an organization (e.g. record or procedure) and the medium on which it is contained.

2.23 Effectiveness

Extent to which planned activities are realized and anticipated results achieved.

2.24 Essential Operations

Activities that are necessary for the organization to meet its business objectives.

2.25 Exercise

Controlled activity to train for, assess, practice, and improve business continuity performance.

2.26 Exercise Plan

Documented information identifying series of exercises designed to meet an overall objective or goal.

2.27 Incident

Event or situation that deviates from what is standard, normal or expected.

2.28 Information

Data processed, organized and correlated to produce meaning.

2.29 Interested Party

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

2.30 Internal Audit

Audit conducted by, or on behalf of, an organization itself for management review or other internal purposes.

2.31 Issue

Important topic, problem or challenge likely to influence an organization's essential operations.

2.32 Likelihood

Chance of occurrence.

2.33 Management Review

Systematic evaluation by top management to determine the suitability, adequacy and effectiveness of the management system to achieve business continuity objectives.

2.34 Management System

Set of interrelated or interacting elements of an organization to establish policies and objectives, and processes to achieve those objectives.

2.35 Measurement

Determination of value.

2.36 Monitoring

Determination of the status of a system, process, product, service or activity.

2.37 Nonconformity

Non-fulfilment of a requirement.

2.38 Objective

Target or goal that an organization sets itself to achieve.

2.39 Organization

Person or group of people with responsibilities, authorities and relationships to achieve targets or goals.

2.40 Performance

Measurable result.

2.41 Post-Exercise Report

Documented information summarizing exercise outcomes.

2.42 Prioritized Activities

Activities to which priority is given during a disruption.

2.43 Procedure

Documented information specifying way to carry out a process or activity.

2.44 Process

Set of interrelated or interacting activities which transforms inputs into outputs.

2.45 Record

Documented information stating results achieved or providing evidence of activities performed.

2.46 Recovery Time Objective (RTO)

Period of time at or within which an activity must be resumed.

2.47 Requirement

Stated or generally implied obligation.

2.48 Risk

Level of uncertainty.

2.49 Risk Assessment

Overall process of risk identification, risk analysis and risk evaluation.

2.50 Risk Criteria

Terms of reference for evaluating the significance of risk.

2.51 Test

Controlled activity to determine if a specific outcome is achievable.

2.52 Threat

Potential cause of disruption.

2.53 Top Management

Person or group of people who direct or lead an organization at the highest level.

2.54 Training

Facilitation of learning and development of competence.

2.55 Verification

Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.

2.56 Vulnerability

Weakness that can be exploited or triggered.

3 GOVERNANCE FRAMEWORK

3 GOVERNANCE FRAMEWORK

Implementation of the management system requires accountabilities, responsibilities and roles to be assigned.

There is no clear endpoint for implementing and maintaining a management system but the similarities with managing a project are such that the roles required for effective project management can also be applied to management systems. Some organizations may not have a person designated for each role and the responsibilities associated with the role may just be added to a person's other responsibilities. Individual titles, for example, BCM manager, BCM representative and group titles, such as, steering committee, may be appropriate in some organizations, but are not necessary.

To be effective, the management system needs to reflect the organization's environment and circumstances and be embedded in the organization's day-to-day operations.

3.1 Top management

Top management is responsible for setting the organization's policy for business continuity (Clause 5.1) and accountable for ensuring that:

a. The management system complies to the requirements of this document and achieves the purpose of the Standard.

b. A governance framework and reporting structure for the management system is put in place.

c. Responsibilities and authorities for roles are assigned and communicated appropriately.

Top management shall commit to the management system and ensure that management system processes integrate with other business processes. Commitment shall be demonstrated by top management through establishing an effective governance framework and ensuring the timely completion of the following:

- Identifying and addressing the context of the organization (Clause 4).
- Setting policy, scope and objectives for the management system (Clause 5).
- Providing the necessary management system support (Clause 6).
- Creating and maintaining documented information (Clause 7).
- Implementing business continuity management operations (Clause 8).
- Reviewing and evaluating the management system (Clause 9).
- Continual improvement of the management system (Clause 10).

3.2 Management system roles and responsibilities

The organization shall ensure that responsibilities and authorities for relevant roles are assigned and communicated within the organization.

The organization shall assign roles and responsibilities for:

- Establishing the management system (Clauses 3 to 7).
- Implementing business continuity management operations (Clause 8).
- Reporting on the performance of the management system (Clause 9.1).
- Reviewing and continual improvement (Clause 9.3 and 10).

3.3 Management system planning

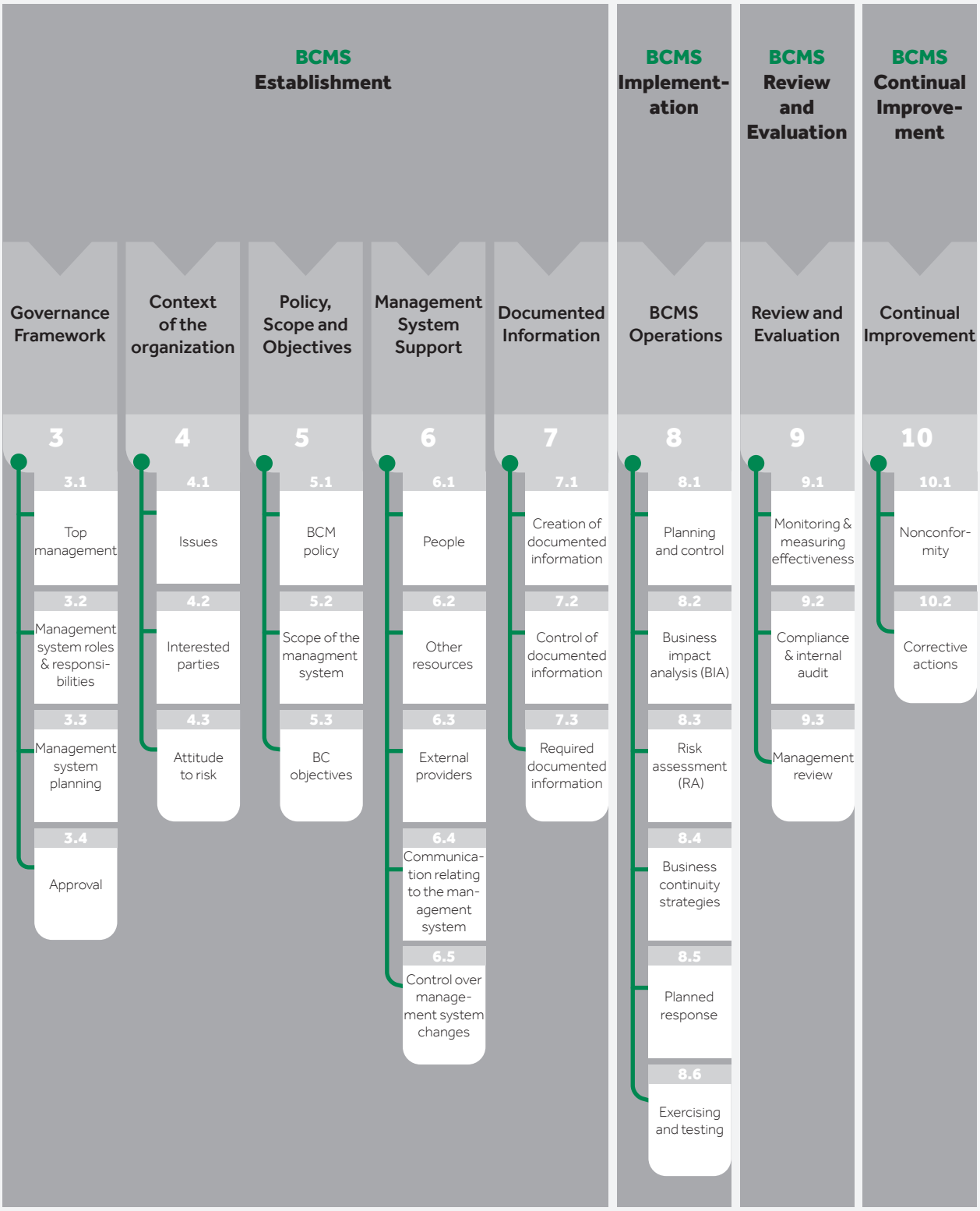


Figure 3: BCMS high level structure (HLS)

The organization shall implement and maintain a management system consisting of processes that integrate with other business processes to achieve business continuity objectives (Clause 5.3) and meet the requirements of this document. All processes required by this document shall be documented (Clause 7).

The organization shall plan how to implement and maintain the management system by determining:

a. The work to be performed.

b. The people (Clause 6.1) and other resources (Clause 6.2) required to undertake the work.

c. Target dates for work completion.

3.4 Approval

Top management shall determine the requirements for approving: Documented information (Clause 7).

4 CONTEXT OF THE ORGANIZATION

4 CONTEXT OF THE ORGANIZATION

Context in this document refers to the environment and circumstances of the organization, including its culture and diversity, its management style, the financial resources available, requirements of interested parties and other issues of relevance. The context determines how the organization will address its needs in relation to:

- Scope, policy and objectives (Clause 5).
- Management system support (Clause 6).
- Documented information (Clause 7).
- Activities and impact criteria used for analysis of business impacts (Clause 8.2).
- Risk parameters and criteria used for the risk assessment (Clause 8.3).
- Evaluation and selection of strategies (Clause 8.4.2).
- The design of response structure (Clause 8.5.2).
- Exercising and testing (Clause 8.6).
- Compliance and internal audit (Clause 9.2).

The organization shall have a process for determining its context.

4.1 Issues

Organizations face challenges, both positive and negative, every day. Understanding the issues and knowing how best to address them is key to an organization's success. External economic and political pressures can influence how the organization sets up the management system and internally, the style of management can have a major bearing. For example, if strong management dictates that certain activities carried out by the organization are essential, then this must be accommodated alongside the requirements of this document.

The organization shall identify issues relevant to its purpose and strategic direction, and business continuity objectives (Clause 5.3).

4.2 Interested parties

Interested parties, commonly referred to as stakeholders, are people or organizations who may be significantly affected by your organization's situation. Understanding what they need and expect from your organization is an important first step in making sure that the management system achieves its purpose. Organizations that manage their relationships with interested parties to minimize the impact of disruptions are undoubtedly more successful than those who do not.

The organization shall identify interested parties and determine their needs and expectations, including legal and regulatory requirements relevant to the organization's business operations.

4.3 Attitude to risk

Determining and setting out how much risk the organization is prepared to take is an important prerequisite for subsequent decision-making. This applies to many aspects of the management system but is particularly relevant to business impact analysis (Clause 8.2), risk assessment (Clause 8.3) and the selection of business continuity strategies (Clause 8.4.2).

Top management shall determine the level and type of risk that the organization will take and ensure that risk criteria is developed and communicated to the organization and its interested parties.

5 POLICY, SCOPE AND OBJECTIVES

5 POLICY, SCOPE AND OBJECTIVES

5.1 Business continuity policy

The business continuity policy sets out top management's intention and direction for the management system and provides a framework for subsequent decision-making, including setting scope and objectives.

Producing a statement that sets out clearly the organization's business continuity policy, scope and objectives is an efficient and effective way of ensuring that staff, customers and other interested parties understand top management's intentions.

The organization shall establish a business continuity policy that is appropriate to the context of the organization (Clause 4) and includes commitment to:

a. Achieving the purpose of the Standard (Clause 1.1).

b. Satisfying the needs and expectations of interested parties (Clause 4.2).

c. Meeting in full, the requirements of this document.

The organization shall create and maintain as documented information, a statement that sets out the organization's business continuity policy, scope of the management system (Clause 5.2) and business continuity objectives (Clause 5.3). The statement shall be communicated to all people under the organization's control and made available to other interested parties, as approved by top management.

5.2 Scope of the management system

The scope explains to interested parties the coverage of the management system so that they can determine if it meets their needs. If products and services or parts of the organization are excluded, the exclusions must be explained and justified to provide assurance that they will not undermine the organization's business continuity.

The organization shall have a process for defining the scope of the management system in-terms of the products and services to be included.

The scope shall be appropriate to the context of the organization (Clause 4) and identify the boundaries and applicability of the management system.

If there are exclusions from scope, these shall be identified, explained and justified. Such exclusions shall not adversely affect the organization's ability to meet the business continuity requirements of its in-scope products and services.

Claiming compliance to this document is only achieved when all requirements applicable to the delivery of products and services within scope are met and are not undermined by a requirement being deemed not applicable.

5.3 Business continuity objectives

The organization needs to explain to staff, customers and other interested parties, its reasons for investing in the management systems and what it expects to achieve.

The organization shall have a process for setting business continuity objectives that explain to interested parties the purpose of the management system.

The process shall ensure that these objectives align with business continuity policy (Clause 5.1), are measurable and are communicated throughout the organization.

6 MANAGEMENT SYSTEM SUPPORT

6 MANAGEMENT SYSTEM SUPPORT

Management systems are effective because they require:

- The management system to be planned.
- Management system processes to be integrated with other business processes.
- The commitment of top management.
- The resources necessary to achieve business continuity objectives.
- Effective communication with external providers.
- People performing key roles to have the necessary competence.
- The workforce to know their role in what the organization is trying to achieve.
- Changes to the management system to be controlled.
- Suitable documentation and records to be retained.

6.1 People

The organization needs to have enough people with the necessary competence to carry out the work required. Otherwise, the organization will not achieve its objectives.

The organization shall determine and provide people with the necessary competence.

6.1.1 Competence

People with management system responsibilities must have the competence necessary to perform their duties effectively. If they don't, the management system will not be successful.

The organization shall have a process for managing the competence of people working under its control.

The process shall include:

a. Determining the competences required for each role.

b. Identifying how competence will be demonstrated.

c. Determining actions required to acquire the necessary competence.

d. Evaluating the effectiveness of actions taken.

6.1.2 Awareness

It is essential that the organization's workforce has decent business continuity awareness and can contribute to achieving management's objectives. The workforce also needs to understand what business continuity is and how it will be implemented before and following the onset of a disruption.

The organization shall have a process for ensuring that all people under its control have sufficient business continuity awareness to understand:

a. The business continuity policy (Clause 5.1) and objectives (Clause 5.3).

b. The meaning of business continuity and its value to the organization.

c. The organization's expectations of them regarding business continuity.

d. Their management system responsibilities, including those for BCMS operations (Clause 8).

e. Threats and risks of disruptions of relevance to them.

f. What to do in the event of a major disruption.

6.2 Other resources

Management system Requirements, including those for responding to disruptions (Clauses 8.5.3.1 to 8.5.3.6), rely on having the necessary resources to ensure that they can be performed.

The organization shall provide other resources needed to operate the management system effectively, including and not limited to adequate provision of:

- Budget allocation.
- Information and data.
- Buildings, facilities and associated utilities.
- Technology equipment and systems.
- Supplies and consumables.
- Logistics, including transportation.
- Other specific requirements.

6.3 External providers

If the organization does not have enough resources internally, it may seek help externally. Where this is done, the organization needs to ensure that the services provided will be of appropriate quality and be available when needed. This can be achieved by putting effective controls in place and making sure that there is effective communication with the external provider.

The organizations shall consider the capabilities and constraints of its internal resources and determine its requirements, if any, for assistance from external providers.

6.3.1 Control of external providers

The organization shall control the work of external providers and ensure that externally provided processes, products and services comply to its requirements. This shall include:

a. Determining and applying criteria for selecting external providers.

b. Treating externally provided processes as being within the management system, including defining the controls to be applied to providers and their output.

6.4 Communication relating to the management system

The organization needs to make sure that it communicates effectively with the interested parties to ensure that they fully understand the purpose of the management system and how they will be affected by it. Communication during disruptions is addressed in (Clause 8).

The organization shall have a process for communicating with interested parties on matters relating to the management system.

The process shall include:

a. Identifying the internal parties with whom to communicate.

b. Identifying the external parties with whom to communicate

c. Determining for each party the information, timing, methods and person to be responsible for communication.

6.5 Control over management system changes

Organizations are constantly changing, so it is important to ensure that mechanisms are in place for detecting the changes, evaluating their impact on the management system and taking appropriate actions.

The organization shall have a process for ensuring that changes affecting the performance of the management system are identified and result in appropriate action being taken.

The process shall include:

a. Identifying changes.

b. Evaluating the effect of the changes on the overall performance of the management system.

c. Determining the actions to be taken.

7 DOCUMENTED INFORMATION

7 DOCUMENTED INFORMATION

The organization needs to explain how processes are performed and result in requirements being met. This is best achieved by writing procedures that describe the processes, including identification of inputs and expected results.

A process usually covers more than one procedure and identifies multiple outputs, many of which are inputs to other processes. Outputs provide a record of how processes are functioning and evidence that requirements are being met.

Documented information is the term used in this document to describe records and procedures that need to be controlled and maintained. Documented information must be locatable, accessible, identifiable, understandable and readable but can be in any format or style that the organization deems acceptable.

7.1 Creation of documented information

The organization shall have a process for creating documented information that provides evidence of processes and compliance of the management system to the requirements of this document, including identification of inputs and intended results. The process shall include:

a. Forms of document identification and a description of its purpose.

b. Documentation formats (e.g. language, software version, graphics).

c. Appropriate media (e.g. paper, electronic).

d. Requirements for review and approval of suitability.

7.2 Control of documented information

The organization shall have a process for controlling and updating documented information to preserve its integrity and ensure that it is identifiable and available at the point of use.
The process shall include controls over:

a. Distribution, access, retrieval and use.

b. Access rights and permissions.

c. Storage and preservation to ensure readability.

d. Updates and versions.

e. Retention and disposal.

f. Determination and labelling of origin.

7.3 Required documented information

The organization shall at minimum create documented information for:

- Management system roles and responsibilities (Clause 3.2) and planning (Clause 3.3).
- Issues, interested parties and attitude to risk (Clause 4).
- Policy, scope and objectives (Clause 5).
- Management system support, including people, other resources, external providers, communication and control over changes (Clause 6).
- BCMS operations including:
    - Planning and control (Clause 8.1).
    - Business impact analysis (Clause 8.2).
    - Risk assessment (Clause 8.3).
    - Business continuity strategies (Clause 8.4).
    - Team structure and composition (Clause 8.5.2).
    - Response requirements (Clause 8.5.3).
    - Exercising and testing plan, post-exercise reports (Clause 8.6).
- Monitoring and measuring effectiveness (Clause 9.1).
- Compliance and audit (Clause 9.2).
- Management review (Clause 9.3).
- Identification of nonconformity (Clause 10.1) and corrective action (Clause 10.2).

The organization shall create and maintain additional documented information that the organization deems necessary for the management system to be effective.

8 BCMS OPERATIONS

8 BCMS OPERATIONS

The management system provides the framework for the organization to establish, review and evaluate business continuity to ensure that it is in line with the policy, scope and objectives (Clause 5).

BCMS operations is the overall process of putting business continuity in place so that the organization can deal with disruptions that might otherwise prevent it from meeting its business objectives.

The organization therefore needs to plan how best to resume activities and reduce the likelihood and impact of disruptions. To achieve this, it needs to:

a. Understand the different impacts that would result from disrupting activities.

b. Identify activities whose disruption would increase the damaging impacts.

c. Prioritise activities and focus the efforts and resources on high priority activities.

d. Evaluate the risks to high priority activities and their dependencies.

e. Identify the resources that high priority activities require for resumption.

f. Plan when and how to resume high priority activities .

The organization's approach to BCMS will depend on its context (Clause 4) and the availability of resources (Clauses 6.1 and 6.2).

8.1 Planning and control

The organization shall plan and implement in a controlled manner, the processes needed for BCMS operations and the resources (Clauses 6.1 and 6.2) to support them.

8.2 Business impact analysis (BIA)

All activities performed by an organization are important, but some need to be given more priority than others during a disruption to ensure that delivery of products and services will continue at an acceptable level. The purpose of the business impact analysis is to identify the organization's high priority activities.

The analysis needs to be based on the organization's unique situation and circumstances and include measurement of the detrimental impacts that would result from its activities being disrupted for differing periods of time. It is not necessary to perform the analysis individually on every activity, it is perfectly acceptable to perform the analysis on groups of activities, for example, relating to specific products.

Differentiating its high priority activities (referred to as 'prioritized activities' in this document) enables the organization to focus on them when considering business continuity strategies.

During the analysis, dependencies of activities need to be identified so that they can be examined as necessary during the risk assessment (Clause 8.3) and also considered when strategies for resuming activities are being investigated.

The analysis also needs to consider the capacity at which activities and their dependencies need to be resumed, bearing in mind that it may not be necessary or appropriate to resume them at their usual capacity. Resumptions at a higher or lower than normal capacity may be appropriate to ensure the necessary product and service delivery. Capacities need further consideration when investigating business continuity strategies (Clause 8.4).

The organization shall have a process for analyzing the business impact of disrupting activities that support delivery of products and services.

The process shall include:

a. Using impact categories and timeframes relevant to the organization's context (Clause 4) to analyse impacts resulting from disruption of activities.

b. Determining the time within which the impacts of not resuming activities would become unacceptable and setting Recovery Time Objectives (RTOs) within that time for their resumption.

c. Determining the capacity at which activities may need to be resumed.

d. Using this analysis results in identifying the organization's 'prioritized activities', which will require business continuity strategies (Clause 8.4) to be in place to ensure their resumption within the predefined RTO.

e. Identifying dependencies of prioritized activities, including people (Clause 6.1), other resources (Clause 6.2), external providers (Clause 6.3) and other activities relied on for delivery of products and services.

Cont. 8.2 **Business impact analysis (BIA)**

Where resumption of a prioritized activity depends on a single external provider, the organization shall evaluate the provider's business continuity arrangements in relation to the dependency and determine the action needed to address any vulnerability.

The output from the BIA shall be in a form suitable for decision-making by top management.

8.3 Risk assessment (RA)

The organization needs to find ways to reduce the risk of disruptions. This can best be achieved by targeting high priority activities and the resources, external providers and other activities they depend on.

The risk assessment provides information that can be used to identify strategies for reducing the likelihood or impact of disruption (Clause 8.4.1).

The organization shall have a risk assessment process that identifies, analyses and evaluates the risk of the organization's prioritized activities being disrupted.

The process shall include:

a. Identification of risks from threats and vulnerabilities that are relevant to the organization's context (Clause 4).

b. Analysis of risks based on consideration of potential causes and sources of risk and their likelihood and anticipated consequences.

c. Evaluation of risks to determine their significance to the organization.

8.4 Business continuity strategies

Having identified its prioritized activities and their dependencies, the organization needs to protect them and try to prevent them from being disrupted. However, because disruptions are inevitable, organizations also need to plan how best to respond to disruptions and resume the activities that have been disrupted.

The organization therefore needs to consider strategies for:

a. Mitigating the risk of prioritized activities being disrupted.

b. Keeping disruption to a minimum.

c. Resuming essential operations within acceptable timeframes.

d. Ensuring effective communication during an incident.

The organization shall have a process for identifying, evaluating, selecting and implementing business continuity strategies. Strategies shall be approved by top management in accordance with requirements applicable (by regulatory or other obligations) and resources needed.

8.4.1 Strategies identification

The organization shall use the outcomes of business impact analysis (Clause 8.2) and risk assessment (Clause 8.3) to identify strategies to achieve:

a. Protecting prioritized activities and reducing the likelihood of disruption.

b. Responding to and shortening the period of disruption.

c. Stabilizing, resuming and recovering prioritized activities.

d. Limiting the impacts of disruption.

8.4.2 Evaluation and selection of strategies and resource requirements

The organization needs to identify and evaluate resources required to implement its selected strategies, these resources include but no limited to:

- People - Where strategies require people to perform specific roles, it is particularly important to identify alternates in case the designated person is not available at the time of the disruption.
- Buildings and facilities.
- Budget allocation.
- Suppliers and service providers.
- Information and communication infrastructure.

The organization shall evaluate and select strategies based on the extent to which they:

a. Enable prioritized activities to resume at agreed capacity within RTO.

b. Align with the amount and type of risk that the organization may or may not take (Clause 4.3).

c. Deliver benefits at manageable and reasonable cost.

The organization shall determine competent people to evaluate and select strategies, people (Clause 6.1) ,other resources (Clause 6.2) and external providers (Clause 6.3) needed to implement selected strategies.

The organization shall specify the resources required to implement the selected strategy, and specify the timing and capacity at which they need to be made available.

8.4.3 Implementation of selected strategies

The organization shall implement and maintain strategies approved by top management.

8.5 Planned response

The organization needs to identify potential disruptions at the earliest opportunity and respond accordingly.

The organization shall have a process for responding to disruptions.

8.5.1 Response teams

Incidents may or may not result in disruption of activities. If the organization is to respond swiftly and decisively to incidents, it needs to have identified in advance people who will perform key roles. Creation of a suitable team structure and selection of suitable team members enables the response to be coordinated and effective.

The organization shall identify teams to be responsible for responding to incidents. The interactions between these response teams shall be clearly stated and for each team, there shall be:

a. Identified people with the necessary responsibility, authority and competence to perform the team's designated role.

b. Documented response Structure (Clause 8.5.2) to guide the team's actions.

8.5.2 Response structure

If teams are to respond effectively, team members must have pre-written structure that provide the information they require and the actions they need to take. It is up to management to choose titles for the structure (e.g. business continuity plan, incident response plan, media response plan, disaster recovery plan) and decide on the number, style and level of detail, all of which need to be suitable for the organization and its workforce.

The structure needs to address all aspects of the organization's response from the detection of an incident through to returning to 'business as usual', including communication during the disruption between all participants. Communicating with interested parties regarding the management system is addressed in (Clause 6.4).

Cont. **8.5.2 Response structure**

The organization shall create and maintain response structure that enable teams to perform their roles.

At minimum, response structure shall address:

a. Command and control (Clause 8.5.3.1).
b. Incident detection and immediate response (Clause 8.5.3.2).
c. Communication during disruptions (Clause 8.5.3.3).
d. Recovery of technology systems (Clause 8.5.3.4).
e. Resumption of prioritized activities (Clause 8.5.3.5).
f. Return to business as normal (Clause 8.5.3.6).

8.5.2 8.5.2.1 Response structure design

Response structure shall:

a. Identify immediate steps to be taken and assist with timely decision-making.
b. Be sufficiently flexible to accommodate unanticipated threats and changeable situations.
c. Focus on anticipated impacts of disruptions.
d. Support strategies that are in place (Clause 8.4.3).
e. Identify roles, tasks and responsibilities.

8.5.2 8.5.2.2 Response structure content

Response Structure shall contain:

a. Purpose and scope of the procedure and team objectives.
b. Roles, responsibilities and authorities.
c. Instructions for team members.
d. Resources needed by the team.
e. Relevant and required reference information.
f. Actions for returning to business as usual.
g. How actions taken and decisions made will be recorded.

8.5.3 Response requirements

8.5.3 8.5.3.1 Command and control

The organization shall define requirements for commanding, controlling and coordinating the organization's response to disruption.

The requirements shall include:

a. Establishing a central team with the capability and authority to make prompt and appropriate decisions and communicate them effectively.

b. Ensuring that information relevant to the disruption is conveyed to the central team in a timely and secure manner.

c. Ensuring timely and secure dissemination of the central team's instructions.

8.5.3 8.5.3.2 Incident detection and immediate response

The organization shall define requirements for detecting potential incidents and responding to disruptions in order to shorten their duration, limit their impact and safeguard those affected. The requirements shall include:

a. Timely detection and assessment of incidents to determine their nature and potential consequences.

b. Assessing threats to human life and damage to infrastructure and services.

c. Using predefined criteria to declare a disruption and initiate an appropriate response.

d. Establishing priorities (giving immediate priority to life safety).

e. Determining actions to be taken to shorten the period and limit the impacts of disruption.

f. Monitoring the consequences of the disruption and the organization's response.

g. Communicating with relevant interested parties, authorities and the media.

h. Creating evacuation procedures and identifying assembly points.

i. Providing first aid and essential supplies.

j. Locating people under the organization's control, including visitors.

k. Assessing potential opportunities for restoration of damaged facilities, equipment and documented information.

8.5.3 8.5.3.3 Communication during disruptions

The organization shall define requirements for ensuring that there is effective communication during a disruption:

a. Between teams and others responding to disruptions.

b. With interested parties.

c. With external providers.

The requirements shall include:

a. Identifying what, when and with whom to communicate.

b. Setting authority levels for communication.

c. Determining how to respond to communications from interested parties.

d. Facilitating structured communication with emergency responders.

e. Ensuring that contact details for all people and organizations identified in response procedures are kept up to date

a. Identifying predefined means of communication.

b. Ensuring availability of the means of communication during a disruption.

c. Responding to communications from interested parties.

d. Preparing procedures for communicating with the media.

Requirements for communicating with the media shall include:

a. Identification of potential channels of communication.

b. Identification of appropriate people to represent the organization.

c. Creation of processes for receiving, acknowledging and responding to media enquiries.

d. Integration of the organization's communications procedures and systems with national, regional and global communication systems (if applicable).

e. Preparation and approval of templates for communicating via the media.

8.5.3 8.5.3.4 Recovery of technology systems

Technology systems are at the heart of almost every organization and will usually need to be recovered before activities can be resumed. The term includes but not limited to:

- Equipment and hardware (including personal computers, mobile devices, racks, servers, storage arrays, tape devices, printers, scanners and fixtures).
- Network (including data connectivity and voice services, switches and routers).
- Software (including operating system and application software, links and interfaces between applications and batch processing routines).
- Data (including application data, voice data and other forms of data).
- The physical environment in which equipment is located.

The organization shall clearly define requirements for recovering technology systems during a disruption.

The requirements shall include:

a. Invoking the required technology response and deployment of people.

b. Accessing back-up data and acquiring alternative service provision.

c. Restoring data, information services, communications and support.

d. Identifying when and at what capacity technology requirements will be made available (Clause 8.2).

e. Providing guidance, if appropriate, on priorities for restoration of damaged equipment.

8.5.3 8.5.3.5 Resumption of prioritized activities

The organization shall clearly define requirements for ensuring that prioritized activities can be resumed within their RTOs following the onset of a disruption.

The requirements shall identify:

a. Strategies and resource requirements for resuming activities and their dependencies.

b. Actions to be taken to resume prioritized activities and prevent further disruption.

8.5.3 8.5.3.6 Return to business as normal

The organization shall clearly define requirements for returning to business as normal following a disruption.

The requirements shall identify:

a. The basis on which a decision for returning to normal will be made.

b. Tasks and responsibilities.

c. How activities not identified as prioritized will be resumed and recovered.

d. Document the incident by a post report.

8.6 Exercising and testing

Exercising and testing is essential to provide assurance that strategies and response structure are effective. It is usually not practical to cover everything within a one-year program, so it makes sense to spread the program over several years. The total time needed will depend on factors such as, the size and complexity of the organization, nature of its operations, pace of change and costs involved. A good starting point for any organization is to conduct team walk-throughs of response structure and requirements.

Typically, exercises are effective in developing teamwork, competency, confidence and knowledge of those involved. Tests on the other hand are generally used to determine if a specific outcome is achievable, for example, ensuring that a computer system is capable or not of being recovered within a specific time limit.

8.6.1 Design of exercises and tests

The organization shall have a process for exercising and testing that validates over time the effectiveness of chosen strategies, promotes confidence in response structure and develops teamwork, competence and knowledge of team members.

The process shall include:

a. Use of appropriate and realistic scenarios.

b. Setting clearly defined objectives and assessing the extent to which they have been achieved.

c. Determining the involvement required from external providers (Clause 6.3).

d. Identifying outcomes, including post-exercise reports, and making recommendations for improvement.

e. Identifying criteria for measuring the success of tests and exercises and the adequacy of strategies.

8.6.2 Performing exercises and tests

Exercises and tests shall be performed at planned intervals and when there are significant changes within the organization or the context in which it operates. The organization shall ensure that the exercising and testing does not adversely impact normal business operations.

9 REVIEW AND EVALUATION

9 REVIEW AND EVALUATION

The best way to ensure that business continuity remains appropriate to the needs of the organization is to measure the performance of the management system and make sure that all processes have been implemented and remain effective. Specific performance indicators can be used to measure how effective individual processes are in achieving the desired outcomes. In the context of business continuity, many organizations use risk indicators to measure changes in levels of risk.

Use of such indicators enables top management to be kept informed of the effectiveness of the management system and the extent to which the organization is meeting its business continuity objectives.

9.1 Monitoring and measuring effectiveness

9.1.1 Performance evaluation

The organization shall have a process for evaluating the performance and effectiveness of the management system, including BCMS operations (Clause 8).

The process shall include:

a. Identifying what needs to be monitored and measured.

b. Identifying ways to monitor and measure.

c. Specifying timing and frequency requirements with justification.

d. Analysing, evaluating and reporting the results of monitoring and measurement.

e. Analysing the outcomes of disruptions.

9.1.2 Performance indicators

The organization shall at minimum identify and use performance indicators (e.g. percentage or number completed) to measure the degree of compliance to the following:

a. Roles defined, and responsibilities currently assigned to people (Clause 3.2).

b. Context of the organization (issues, interested parties and attitude to risk) identified, documented and signed off (Clause 4).

c. Statement of policy, scope and objectives created, approved and published (Clause 5).

d. Competencies defined, documented and approved (Clause 6.1.1).

e. Participation of team members in training (Clause 6.1.1) and workforce awareness (Clause 6.1.2).

Cont. **9.1.2 Performance indicators**

f. Business impact analyses completed, documented and approved (Clause 8.2).
g. Risk assessments completed, documented and approved (Clause 8.3).
h. Business continuity strategies documented, selected, approved and in place (Clause 8.4).
i. Team structure defined and positions filled (Clause 8.5.1).
j. Response structure created and approved (Clause 8.5.2).
k. Exercises and tests designed and planned (Clause 8.6.1).
l. Exercises conducted, post-exercise reports produced and approved (Clause 8.6.2).
m. Internal audit coverage of the management system (Clause 9.2).
n. Management review completed within past year (Clause 9.3).
o. Nonconformities with no approved corrective actions (Clause 10).
p. Corrective actions documented, approved and completed (Clause 10.2).

9.2 Compliance and internal audit

Getting an unbiased assessment of the management system is an excellent way of finding out if it has been properly implemented and identifying improvement opportunities. The frequency of audits will be driven by the organization's situation (Clause 4), its BCMS operations (Clause 8) and the results of previous audits.

Effective planning and performance of internal audits is essential to ensure that over a reasonable period of time they cover the entire scope of the management system. The results of internal audits will give top management a picture of the overall effectiveness of the management system and provide the basis for setting continual improvement objectives.

Internal audits may be performed by people from within the organization or outside it. In either case, the auditor needs to be competent and able to conduct the audit impartially and objectively. In smaller organizations it may only be necessary to ensure that the auditor is not actively involved in the activity being audited.

The organization shall have a process for conducting internal audits of the management system at planned intervals to obtain evidence that the management system complies to the requirements of this document and enables the organization to meet its business continuity objectives (Clause 5.3).

Cont. 9.2 Compliance and internal audit

The process shall include:

a. Ensuring that audits are planned, performed and relevant to the requirements of interested parties.

b. Determining the intervals between audits based on the context of the organization.

c. Defining the audit criteria and specifying the scope of each audit.

d. Ensuring the auditor's competence, objectivity and impartiality.

e. Identification of nonconformities and recommendations for improvement based on audit evidence.

f. Effective reporting of audit findings and conclusions to top management and those responsible for the management system processes examined.

9.3 Management review

Involving top management in reviews of the management system promotes confidence, and demonstrates the management's commitment to keeping business continuity as a priority for the organization.

9.3.1 Timing and purpose of management review

The organization shall have a process for top management to review the management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness including the effectiveness of its strategies (Clause 8.4) and response structure (Clause 8.5.2).

The process shall include:

a. Conducting reviews at least annually and when significant changes occur.

b. Identifying the status of actions agreed at previous management reviews.

c. Reviewing top management's accountabilities and commitments (Clause 3.1).

d. Assessing the impact of context changes (Clause 4) on the management system.

e. Reviewing feedback from interested parties (Clause 4.2).

f. Assessing the need for changing policy, scope or objectives (Clause 5).

g. Reviewing evaluations of the performance and effectiveness of the management system (Clause 9.1).

h. Examining trends relating to:

- Analysis and evaluation of the results of monitoring and measurement (Clause 9.1).
- Audit results (Clause 9.2).
- Nonconformities (Clause 10.1) and corrective actions (Clause 10.2).

9.3.2 Outcome of management review

The organization shall retain documented information of the outcome of the management review which defines appropriate actions to improve the suitability, adequacy and effectiveness of the management system.

Based on the outcome of the management review, top management shall agree on actions necessary to improve the suitability, adequacy and effectiveness of the management system.

10 CONTINUAL IMPROVEMENT

10 CONTINUAL IMPROVEMENT

The purpose of continual improvement is to take the management system to a higher level of efficiency and effectiveness by reacting to nonconformity and implementing corrective actions to address it.

10.1 Nonconformity

There will inevitably be occasions when requirements are not fulfilled, and weaknesses come to light. In a well-designed management system that operates effectively, such problems will be highlighted so that they can be investigated, their root cause identified and addressed by corrective action (Clause 10.2).

Nonconformities are often identified during internal audits (Clause 9.2) or by people with management system responsibilities but may also be highlighted by performance indicators (Clause 9.1.2) or analysis of industry trends and events.

The organization shall have a process for identifying nonconformities and taking action to control and correct them.

The process shall include:

a. Reviewing the nonconformity to determine its cause.

b. Determining if similar nonconformity exists or could occur.

c. Taking appropriate corrective actions.

d. Changing the management system as necessary.

e. Recording the results and reviewing the effectiveness of corrective action taken.

10.2 Corrective actions

Corrective actions address deficiencies in the management system and ensure that it functions as intended.

The organization shall have a process for taking corrective action in a timely manner to eliminate the causes of nonconformity and to prevent its recurrence.

Corrective action shall be appropriate to the effects and consequences of the nonconformity encountered.