DRAFT INTERNATIONAL STANDARD ISO/DIS 22301

ISO/TC **223** Secretariat: **SIS**

Voting begins on
2010-11-26

Voting terminates on
2011-04-26

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

Societal security — Preparedness and continuity management systems — Requirements

Sécurité sociétale — État de préparation et systèmes de gestion de la continuité — Exigences

ICS 03.100.01

In accordance with the provisions of Council Resolution 15/1993 this document is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 15/1993, ce document est distribué en version anglaise seulement.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Contents

Page

Foreword v

Introduction vi
0.1 General vi
0.2 The Plan-Do-Check-Act (PDCA) cycle vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 General requirements 6
4.1 Understanding of the organization and its context 6
4.2 Needs and requirements 6
4.3 Management system and scope 6

5 Leadership 6
5.1 General 6
5.2 Management commitment 7
5.3 Policy 7
5.4 Organizational roles, responsibilities and authorities 7

6 Planning 8
6.1 Objectives and plans to achieve them 8
6.2 Action to address issues and concerns 8

7 Support 9
7.1 Resources 9
7.2 Competence 9
7.3 Awareness 9
7.4 Communication 9
7.4.1 External communication 9
7.4.2 Internal communication 9
7.5 Documented information 9
7.5.1 General 9
7.5.2 Create and update 10
7.5.3 Control of documented Information 10

8 Operation 10
8.1 General 10
8.2 Operational planning and control 11
8.3 Preparation 11
8.4 Planning 12
8.4.1 Management commitment 12
8.4.2 Policy development 12
8.4.3 Business impact analysis and risk assessment 13
8.4.4 Business continuity options 14
8.5 Performing 15
8.5.1 Developing and implementing a business continuity response 15
8.5.2 Response structure 15
8.5.3 Warning and communication 16
8.5.4 Response 16
8.5.5 Business continuity plans 17
8.5.6 Response procedure requirements 17
8.5.7 Response procedure content 17
8.5.8 Recovery 18

8.5.9 Communication and consultation 18
8.6 Checking 19
8.6.1 Exercising and testing 19
8.6.2 Monitoring performance 19
8.7 Reviewing 19
8.7.1 Management review 19
8.7.2 Evaluation of continuity procedures 20

9 Performance evaluation 21
9.1 Monitoring and measurement 21
9.2 Internal audit 21
9.3 Management review 22

10 Improvement 22
10.1 Nonconformity and corrective action 22
10.2 Continual improvement 23

Bibliography 24

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

ISO 22301 was prepared by Technical Committee ISO/TC 223, *Societal security*.

Introduction

General

This International Standard specifies requirements for setting up and managing an effective Business Continuity Management System (BCMS).

This emphasizes the importance of:

a) understanding continuity and preparedness needs and the necessity for establishing business continuity management policy and objectives;

b) implementing and operating controls and measures for managing an organization's overall continuity risks;

c) monitoring and reviewing the performance and effectiveness of the BCMS; and

d) continual improvement based on objective measurement.

A BCMS, like any other management system, has the following key components

e) a policy;

f) people with defined responsibilities;

g) management processes relating to:

   1) policy;

   2) planning;

   3) implementation and operation;

   4) performance assessment;

   5) management review; and

   6) improvement;

h) a set of documentation providing auditable evidence; and

i) any business continuity management processes relevant to the organization.

The Plan-Do-Check-Act (PDCA) cycle

The standard applies the “Plan-Do-Check-Act” (PDCA) cycle to planning, establishing, implementing, operating, monitoring, reviewing, exercising, maintaining and continually improving the effectiveness of an organization’s BCMS.

This ensures a degree of consistency with other management systems standards, such as ISO 9001:2008 (Quality Management Systems), ISO 14001:2004 (Environmental Management Systems), ISO/IEC 27001:2005 (Information Security Management Systems) and ISO/IEC 20000-1:2005 (Information

Technology - Service Management), thereby supporting consistent and integrated implementation and operation with related management systems (see Annex A).

Figure 1 illustrates how a BCMS takes as inputs stakeholders' requirements for continuity management and, through the necessary actions and processes, produces continuity outcomes (i.e. managed continuity) that meet those requirements.

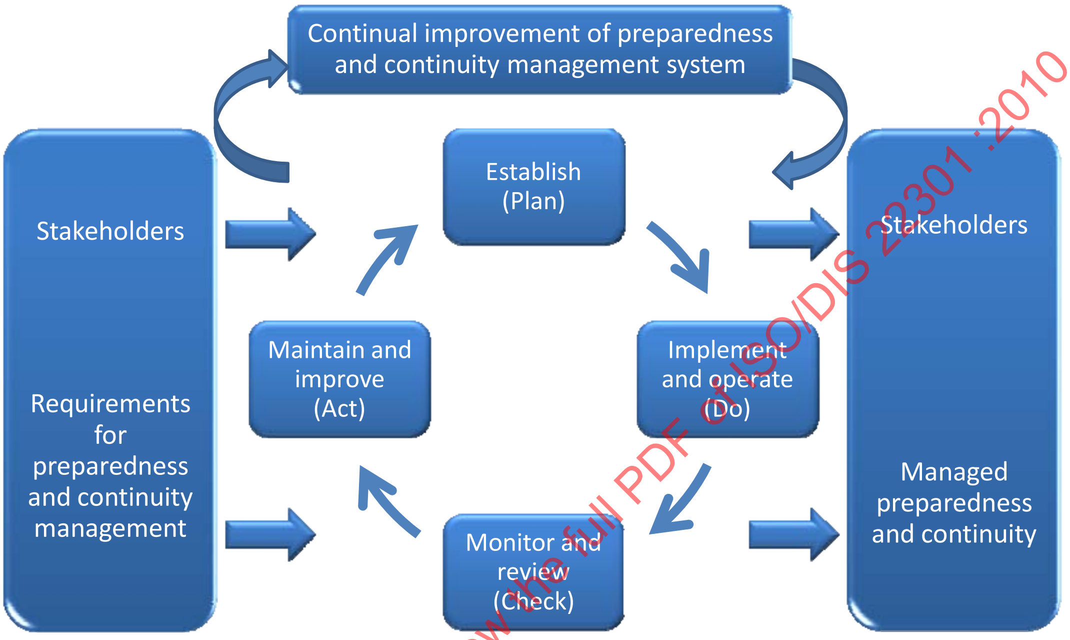
Continual improvement of preparedness and continuity management system
Stakeholders
Requirements for preparedness and continuity management
Establish (Plan)
Maintain and improve (Act)
Implement and operate (Do)
Monitor and review (Check)
Stakeholders
Managed preparedness and continuity

Figure 1 — PDCA cycle applied to BCMS processes

Societal security — Preparedness and continuity management systems — Requirements

1 Scope

This International Standard for business continuity specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to prepare for, respond to and recover from disruption.

The requirements specified in this International Standard are generic and intended to be applicable to all organizations (or parts thereof), regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity.

It is not the intent of this International Standard to imply uniformity in the structure of a Business Continuity Managament System (BCMS), but for an organization to design a BCMS that is appropriate to its needs and that meets its stakeholders' requirements. These needs are shaped by regulatory, organizational and industry requirements, the products and services, the processes employed, the size and structure of the organization, and the requirements of its stakeholders.

This International Standard is applicable to all types and sizes of organizations that wish to:

a) establish, implement, maintain and improve a BCMS;

b) assure conformance with stated BCMS policy;

c) demonstrate conformance to others;

d) seek certification/registration of its BCMS system by an accredited third party certification body; or

e) make a self-determination and self-declaration of conformance with this International Standard.

This International Standard can be used to assess an organization's ability to meet its own continuity needs and obligations.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced (including any amendments) applies.

ISO/IEC Guide 73: 2009, *Risk management — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC Guide 73:2009 and the following apply.

3.1
audit
process for obtaining evidence and assessing it objectively to determine the extent to which specified requirements are fulfilled

3.2
business continuity management
management process which provides a framework for building capability that safeguards the objectives of the organization including its obligations.

3.3
business impact analysis
process of analysing business functions and the effect at the business disruption might have upon them

3.4
competence
demonstrated ability to apply knowledge and skills to achieve intended results

3.5
conformity
fulfilment of a requirement

3.6
continual improvement
recurring activity to enhance performance

3.7
correction
action to eliminate a detected nonconformity

3.8
corrective action
action to eliminate the cause of a nonconformity or other undesirable situation and to prevent recurrence

3.9
document
information and its supporting medium

NOTE 1 The medium can be paper, magnetic, electronic or optical computer disc, photograph or master sample, or a combination thereof

NOTE 2 A set of documents, for example specifications and records, is frequently called “documentation”

3.10
effectiveness
extent to which planned activities are realized and planned results achieved

3.11
efficiency
relationship between the result achieved and the resources used

3.12
event
occurrence or change of a particular set of circumstances

NOTE 1 An event can be one or more occurrences, and can have several causes.

NOTE 2 An event can consist of something not happening.

NOTE 3 An event can sometimes be referred to as an “incident” or "accident".

NOTE 4 An event without consequences may also be referred to as a "near miss", “incident”, "near hit", "close call".

[ISO/IEC GUIDE 73]

3.13
exercise
Instrument to train for, assess, practice, and improve performance and capabilities in a controlled environment

NOTE A test is a unique and particular type of exercise, which incorporates an expectation of a pass or fail element within the aim or objectives of the exercise being planned

3.14
infrastructure
system of facilities, equipment and services needed for the operation of an organization

3.15
interested party
affected party with an interest in the success of an organization or an activity

3.16
management system
set of interrelated or interacting elements to establish policies and objectives, and processes to achieve those objectives

NOTE An organization’s management system can address a limited field, such as quality or environment. A management system that merges more than one field, is referred to as an “integrated management system”.

3.17
monitoring
planned observation of performance

3.18
mutual aid agreement
a pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement

3.19
nonconformity
non-fulfilment of a requirement

3.20
objective
desired outcome set by the organization

3.21
operations control
process, practice, or other actions that assure management outcomes

3.22
operations planning
scheme specifying the approach, the management elements and resources to be applied to management of the organization

3.23
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

NOTE 1 The concept of organization includes, but is not limited to company, corporation, firm, enterprise, authority, partnership, sole-trader, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

NOTE 2 For organizations with more than one operating unit, a single unit may be defined as an organization.

3.24
performance
measurable outcome

NOTE 1 Performance can relate to activities, processes, systems and products.

NOTE 2 Performance includes not only the resulting extent of progress against objectives, but can also include the extent of progress in implementing a management system.

3.25
performance evaluation
process of determining measurable results

3.26
personnel
people working for and under the control of the organization

NOTE The concept of personnel includes, but is not limited to employees, part-time staff, and agency staff.

3.27
policy
intentions and direction of an organization as formally expressed by top management

3.28
prevention
measures that enable an organization to avoid a potential disruption

3.29
preventive action
action to reduce or eliminate risk

3.30
procedure
specified way to carry out an activity or a process

3.31
protection
measures that enable an organization to avoid, preclude, or limit the likelihood or consequences of a disruption

3.32
prioritized activities
activities to which urgent priority must be given following an incident in order to mitigate impacts

NOTE Terms in common use to describe activities within this group include: critical, essential, vital, urgent and key.

3.33
record
statement of results achieved or evidence of activities performed

3.34
requirement
need or expectation that is stated, generally implied or obligatory

3.35
risk
effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected — positive and/or negative.

NOTE 2 Uncertainty is the state, even partial, of deficiency of information related to an event. The combination of consequence and likelihood of an event can be used to characterize risk.

NOTE 3 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

3.36
risk appetite
amount and type of risk that an organization is prepared to seek, accept or tolerate

3.37
risk source
element which alone or in combination has the intrinsic potential to give rise to risk

NOTE A risk source can be tangible or intangible.

[ISO/IEC GUIDE 73]

3.38
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

NOTE A decision maker can be a stakeholder.\

3.39
test
see: testing

3.40
testing
procedure for evaluation; a means of determining the presence, quality, or veracity of something

NOTE 1 Testing may be referred to a “trial”.

NOTE 2 Testing is often applied to supporting plans.

3.41
top management
person or group of people who directs and controls an organization at the highest level

3.42
verification
confirmation, through the provision of evidence, that specified requirements have been fulfilled

3.43
work environment
set of conditions under which work is performed

NOTE Conditions include physical, social, psychological and environmental factors (such as temperature, recognition schemes, ergonomics and atmospheric composition).

4 General requirements

4.1 Understanding of the organization and its context

The organization shall determine external and internal factors that are relevant to its purpose and that affect its ability to achieve the expected outcomes of its BCMS.

These factors shall be taken into account when establishing, implementing and maintaining the organization's BCMS, and assigning priorities.

NOTE Organizations of all types, size and complexity operate in circumstances that are subject to opportunities, change and risk, consequently the organization evaluates such information in order to innovate, maintain and/or improve the effectiveness of its management system, during its short-term and long-term planning.

4.2 Needs and requirements

When establishing its BCMS, the organization shall determine:

— its relevant interested parties; and

— their needs and requirements, including applicable legal requirements.

NOTE The balancing of needs can be achieved by an organization by giving due weight to the needs of interested parties, for example, consumers, owners, society etc.

4.3 Management system and scope

The organization shall establish, implement, maintain and improve a BCMS in accordance with the requirements of this International Standard.

The organization shall consider:

— the external and internal factors referred to in 4.1;

— the needs and requirements referred to in 4.2,

and determine issues or concerns to:

— assure the management system can achieve its expected outcome(s);

— prevent undesired effects;

— address opportunities for improvement.

The organization shall define and retain documented information on the scope of the BCMS, such that the boundaries and applicability of the BCMS can be clearly communicated to internal and external parties.

5 Leadership

5.1 General

Top management shall demonstrate leadership with respect to the BCMS by:

— visibly directing and controlling its overall direction and operation;

- motivating persons to ensure the BCMS supports the business continuity performance of the organization.

NOTE Leadership is not restricted to just top management.

5.2 Management commitment

Top management shall demonstrate its commitment by:

- ensuring the BCMS is compatible with the strategic direction of the organization;
- integrating the BCMS requirements into the organization's business processes;
- providing the resources to establish, implement, maintain and continually improve the BCMS (see 7.1);
- communicating the importance of effective Business Continuity Management and conformance to the BCMS processes;
- performing effective management reviews to ensure that the BCMS achieves its expected outcomes;
- directing and supporting continual improvement.

NOTE Reference to “business” in this international standard should be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

5.3 Policy

Top management shall establish and communicate a Business Continuity policy. The policy shall:

a) be appropriate to the purpose of the organization;

b) provide the framework for setting objectives;

c) include a commitment to satisfy applicable needs and requirements,

d) include a commitment to continual improvement of the BCMS;

e) be implemented;

f) be reviewed for continuing suitability; and

g) be available to interested parties.

The organization shall retain documented information on the policy.

5.4 Organizational roles, responsibilities and authorities

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

Top management shall assign the responsibility and authority for:

a) ensuring that the management system is established and implemented in accordance with the requirements of this International Standard;

b) reporting on the performance of the BCMS to top management.

6 Planning

6.1 Objectives and plans to achieve them

Top management shall ensure that objectives are established for relevant functions and levels within the organization.

The objectives shall:

- be consistent with the policy;
- be measurable (if practical);
- have time frames for their achievement;
- take account of applicable needs and requirements;
- enable opportunities to maintain or improve performance;
- be monitored and updated as appropriate.

The organization shall retain documented information on the objectives.

To achieve its objectives, the organization shall determine:

a) who is responsible;

b) what will be done, and when it will be completed;

c) how the results will be evaluated.

6.2 Action to address issues and concerns

The organization shall determine how to address the issues and concerns identified in 4.3 that may affect its ability to achieve the expected outcomes of the BCMS.

The organization shall:

a) evaluate the need to plan action to address these issues and concerns;

b) if necessary:

    1) integrate and implement these actions into its BCMS processes,

    2) ensure information will be available to evaluate if the actions have been effective (see 9.1).

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the BCMS.

7.2 Competence

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its performance

b) ensure these persons are competent on the basis of appropriate education, training, and experience,

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken

d) retain appropriate documented information as evidence of competence and any actions taken.

NOTE Applicable actions may include the provision of training, the hiring of new persons, or the contracting of competent persons

7.3 Awareness

Persons doing work under the organization’s control shall be aware of:

- the business continuity management policy;
- their contribution to the effectiveness of the BCMS, including the benefits of improved business continuity management performance;
- the effects of their divergence from the BCMS requirements.

7.4 Communication

7.4.1 External communication

The organization shall establish, implement and maintain arrangements for communicating with relevant external interested parties.

7.4.2 Internal communication

The organization shall establish, implement and maintain arrangements for internal communication within the organization.

7.5 Documented information

7.5.1 General

The organization’s BCMS shall include:

- documented information required by this International Standard;
- documented information determined by the organization as being required for the effectiveness of the BCMS.

7.5.2 Create and update

The process for creating or updating documented information (see 7.5.1) shall include:

a) its identification and description (e.g. a title, name, date, author, number, revision reference etc.);

b) consideration of how the information will be captured and presented;

c) its review and approval for adequacy, when applicable.

NOTE 1 The capture and presentation includes what format is to be used (e.g. language, software version, graphics) or media is to be used (e.g. paper, electronic document).

NOTE 2 The extent of documented information for a BCMS can differ from one organization to another due to:

— the size of organization and its type of activities, processes, products and services,

— the complexity of processes and their interactions, and

— the competence of persons.

7.5.3 Control of documented Information

Documented information required by the BCMS and by this International Standard shall be controlled.

Controls for documented information shall include as applicable:

a) distribution;

b) access;

c) storage and preservation;

d) retrieval and use;

e) identification of version and changes;

f) preservation of legibility (i.e. clear enough to read);

g) prevention of the unintended use of obsolete information;

h) retention and disposition.

Ensure that documented information of external origin determined by the organization to be necessary for the planning and operation of the BCMS is identified as appropriate, and controlled.

8 Operation

8.1 General

Unlike the previous chapters, this chapter follows the unified approach for a management system standard only in 8.1. From 8.2 onwards, the specific requirements for business continuity are defined.

8.2 Operational planning and control

The organization shall determine, plan, implement and control those operational activities needed to:

- fulfil its BCMS policy and objectives;

- meet applicable needs and requirements.

This shall include:

a) establishing criteria for those activities and/or processes;

b) implementing controls, in accordance with the criteria;

c) keeping documented information to demonstrate that the activities and/or processes have been carried out as planned.

The organization shall ensure that planned changes are controlled and that unintended changes are reviewed and appropriate action is taken.

NOTE Operational activities and/or processes may include activities and/or processes that are contracted out or outsourced, or related to the supply of goods and services.

8.3 Preparation

The organization shall identify and document the following in defining the context for the management system and its commitment to business continuity management within specific internal and external contexts of the organization:

a) the organization's activities, functions, services, products, partnerships, supply chains, stakeholder relationships, and the potential impact related to a disruptive incident;

b) links between the business continuity policy and the organization's objectives and other policies, including its overall risk management strategy;

c) the organization's risk appetite.

In establishing the context, the organization shall:

d) articulate its objectives, including those concerned with Business Continuity

e) identify its stakeholders and their objectives;

f) define the external and internal factors that create the uncertainty that gives rise to risk;

g) set risk criteria; and

h) define a scope and purpose of the particular risk management activity.

The organization shall define and document the scope of the BCMS, considering its internal and external context.

The organization shall:

i) establish the parts of the organization to be included in the BCMS;

j) establish BCMS requirements, considering the organization's mission, goals, internal and external obligations (including those related to stakeholders), and legal responsibilities;

k) identify products and services and all related activities within the scope of the BCMS;

l) take into account stakeholders needs and interests, such as customers, investors, shareholders, the supply chain, public and/or community input and needs, expectations and interests (as appropriate);

m) define the scope of the BCMS in terms of and appropriate to the size, nature and complexity of the organization.

When defining the scope, the organization shall document any exclusions; any such exclusions do not affect the organization's ability and responsibility to provide continuity of business and operations that meet the BCMS requirements, as determined by impact analysis or risk assessment and applicable legal or regulatory requirements.

8.4 Planning

8.4.1 Management commitment

Top management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the BCMS by:

a) establishing a business continuity management policy;

b) ensuring that BCMS objectives and plans are established;

c) establishing roles, responsibilities, and competencies for business continuity management;

d) appointing one or more persons to be responsible for the BCMS with the appropriate authority and competencies to be accountable for the implementation and maintenance of the BCMS;

NOTE These persons may hold other responsibilities within the organization

e) communicating and promoting awareness within the organization of the importance of meeting business continuity management objectives and conforming to business continuity management policy, its responsibilities under the law, and the need for continual improvement;

Top management shall ensure that the responsibilities and authorities for relevant roles as assigned and communicated within the organization by:

f) providing sufficient resources to establish, implement, operate, monitor, review, maintain, and improve the BCMS;

g) defining the criteria for accepting risks and the acceptable levels of risk;

h) actively engaging in exercising and testing;

i) ensuring that internal audits of the BCMS are conducted;

j) conducting management reviews of the BCMS;

k) demonstrating its commitment to continual improvement.

8.4.2 Policy development

Top management shall define the business continuity management policy in terms of the organizations objectives and its obligations.

The policy shall be:

a) approved by top management;

b) communicated to all persons working for or on behalf of the organization deemed within the scope of the BCMS;

c) available to stakeholders as approved by management;

d) reviewed at defined intervals and when significant changes occur.

8.4.3 Business impact analysis and risk assessment

8.4.3.1 General

The organization shall establish, implement and maintain a formal and documented process for business impact analysis and risk assessment that:

a) establishes the context of assessment, defines criteria and evaluates the potential impact related to a disruptive incident;

b) includes systematically defined criteria for evaluating the potential impacts of disruptive incidents;

c) takes into account legal and other requirements to which the organization subscribes;

d) includes systematic analysis, prioritization of risk controls and treatments, and their related costs;

e) defines the required output from the business impact analysis and risk assessment; and

f) specifies the requirements for this information to be kept up-to-date and confidential.

NOTE There are various methodologies for business impact analysis and risk assessment which will determine the order in which these will be conducted.

8.4.3.2 Legal and other requirements

The organization shall establish, implement and maintain a procedure(s) to identify, have access to, and assess the applicable legal requirements and other requirements to which the organization subscribes related to the continuity of its operations, products and services, as well as the interests of relevant stakeholders.

The organization shall ensure that these applicable legal requirements and other requirements to which the organization subscribes are taken into account in establishing, implementing and maintaining its Business Continuity Management system.

The organization shall document this information and keep it up-to-date. New or variations to legal and other requirements shall be communicated to affected employees and other stakeholders.

8.4.3.3 Business impact analysis

The organization shall establish, implement, and maintain a formal and documented evaluation process for determining continuity and recovery priorities, objectives and targets. This process shall include assessing the impacts of disrupting activities that support the organization's products and services.

The business impact analysis shall include the following:

a) identifying activities that support the provision of products and services;

b) assessing over time the impacts of not performing these activities;

c) setting prioritized timeframes for resuming these activities at a specified minimum acceptable level, taking into consideration the time within which the impacts of not resuming them would become unacceptable;

d) identifying dependencies and supporting resources of these activities, including suppliers, outsource partners and other relevant stakeholders.

8.4.3.4 Risk assessment

The organization shall establish, implement, and maintain a formal documented risk assessment process that systematically identifies, analyzes, and evaluates the risk of disruptive events to the organization. This process shall be made in accordance with ISO 31000.

The organization shall:

a) identify risks of disruption to the organization's prioritized activities and the processes, systems, information, people, assets, outsource partners and other resources that support them;

b) systematically analyze risk;

c) evaluate which disruption related risks require treatment; and

d) identify treatments commensurate with business continuity and recovery objectives and in accordance with the organization's risk appetite.

NOTE The organization should be aware that certain financial or governmental obligations require the communication of these risks at varying levels of detail. In addition, certain societal needs may also warrant sharing of this information at an appropriate level of detail.

8.4.4 Business continuity options

8.4.4.1 Determination and selection

Determination and selection of options shall be based on the outputs from the business impact analysis and risk assessment.

The organization shall determine appropriate continuity options for:

a) protecting prioritized activities;

b) stabilising, continuing, resuming and recovering prioritized activities and their dependencies and supporting resources; and

c) mitigating, responding to and managing impacts.

The determination of options shall include setting prioritized time frames for the resumption of activities within their maximum tolerable periods of disruption.

8.4.4.2 Establishing resource requirements

The organization shall determine the resource requirements to implement the selected options. The types of resources considered shall include:

a) people;

b) information and data;

c) buildings, work environment and associated utilities;

d) facilities, equipment and consumables;

e) information technology and telecommunications systems;

f) transportation;

g) finance; and

h) partners and suppliers.

The organization shall choose and implement appropriate recovery strategies and business contingencies to obtain and operate resources required for critical process recovery in accordance with the risk appetite.

8.4.4.3 Protection and mitigation

For identified risks requiring treatment, the organization shall consider proactive measures that:

a) reduce the likelihood of disruption;

b) shorten the period of disruption; and

c) limit the impact of disruption on the organization’s key products and services.

The organization shall choose and implement appropriate risk treatments in accordance with its level of risk acceptance.

8.5 Performing

8.5.1 Developing and implementing a business continuity response

The organization shall establish, implement, and maintain business continuity procedures to manage a disruptive event and continue its activities based on recovery objectives identified in the business impact analysis.

The organization shall document procedures (including necessary arrangements) to ensure continuity of activities and management of a disruptive event.

The procedures shall be:

a) establishing the appropriate internal and external communications protocol;

b) specific regarding the immediate steps that should be taken during a disruption;

c) flexible to respond to unanticipated threat scenarios and changing internal and external conditions;

d) focused on the impact of events that could potentially disrupt operations;

e) developed based on stated assumptions and an analysis of interdependencies; and

f) efective in minimizing consequences through implementation of appropriate mitigation strategies.

8.5.2 Response structure

The organization shall establish, document, and implement procedures and a management structure to prepare for, mitigate, and respond to a disruptive event using personnel with the necessary authority, experience, and competence.

The response structure shall:

a) identify impact thresholds that justify initiation of formal response;

b) assess the nature and extent of a disruptive event or the potential impact;

c) initiate an appropriate business continuity response;

d) have processes, and procedures for the activation, operation, coordination, and communication of the response;

e) have resources available to support the processes and procedures to manage a disruptive event or work to minimize impact before realized; and

f) communicate with stakeholders and authorities, as well as the media.

8.5.3 Warning and communication

The organization shall establish, implement and maintain procedures for:

a) detecting an incident

b) continuing monitoring of incident

c) internal communication between the various levels and functions within the organization;

d) external communications with partner organizations and other stakeholders;

e) receiving, documenting and responding to communication from other stakeholders;

f) receiving, documenting and responding to any national or regional risk advisory system or equivalent;

g) alerting stakeholders potentially impacted by an actual or impending disruptive incident;

h) assuring availability of means of communication during a disruptive incident;

i) facilitating structured communication with emergency responders;

j) assuring the interoperability of multiple responding organizations and personnel;

k) recording of vital information about the incident, actions taken and decisions made; and

l) operations of a communications facility.

The organization shall decide, using life safety as the first priority and in consultation with its stakeholders, whether to communicate externally about its significant risks and impacts and document its decision. If the decision is to communicate then the organization shall establish and implement procedures for this external communication, alerts and warnings including the media as appropriate.

The communication and warning system shall be regularly exercised.

8.5.4 Response

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

The organization shall establish an incident response structure that provides for personnel to:

a) confirm the nature and extent of an incident;

b) trigger an appropriate response;

c) have processes and procedures for the activation, operation, coordination and communication of the incident response;

d) have resources available to support the processes and procedures to manage an incident; and

e) communicate with stakeholders.

8.5.5 Business continuity plans

The organization shall establish documented plans that detail how the organization will manage a disruptive event and how it will recover or maintain its activities to a predetermined level, based on management-approved recovery objectives.

Each plan shall define:

a) purpose and scope;

b) objectives and measures of success;

c) activation criteria and procedures;

d) implementation procedures;

e) roles, responsibilities, and authorities;

f) communication requirements and procedures;

g) internal and external interdependencies and interactions;

h) resource requirements; and

i) information flow and documentation processes.

The organization shall periodically exercise, review, and (where necessary) revise its business continuity plans — in particular, after the occurrence of the disruptive event and its associated post-event review.

8.5.6 Response procedure requirements

The organization shall have documented procedures for responding to a disruptive incident.

Such procedures shall address the requirements of those who will use them and include:

a) initially responding to an incident, assessing the incident and managing any immediate threats;

b) ensuring the organization will have a minimal acceptable capability proportionate to the scope of its BCMS; and

c) the stabilization, continuity and recovery requirements of the organization’s prioritized activities.

8.5.7 Response procedure content

The response procedures shall collectively contain:

a) defined roles and responsibilities for people and teams having authority during and following an incident;

b) a process for activating the response;