INTERNATIONAL STANDARD

ISO 22313

First edition
2012-12-15

Societal security — Business continuity management systems — Guidance

Sécurité sociétale — Systèmes de management de la continuité d'activité — Lignes directrices

Reference number
ISO 22313:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 22313 was prepared by Technical Committee ISO/TC 223, *Societal security*.

For the purposes of research, users are encouraged to share their views on ISO 22313:2012 and their priorities for changes to future editions of the document. Click on the link below to take part in the online survey:

http://www.surveymonkey.com/s/22313

Introduction

General

This International Standard provides guidance, where appropriate, on the requirements specified in ISO 22301:2012 and provides recommendations ('should') and permissions ('may') in relation to them. It is not the intention of this International Standard to provide general guidance on all aspects of business continuity.

This International Standard includes the same headings as ISO 22301 but does not repeat the requirements for business continuity management systems and its related terms and definitions. Organizations wishing to be informed of these must therefore refer to ISO 22301 and ISO 22300.

To provide further clarification and explanation of key points, this International Standard includes a number of figures. All such figures are for illustrative purposes only and the related text in the body of this International Standard takes precedence.

A business continuity management system (BCMS) emphasizes the importance of:

— understanding the organization's needs and the necessity for establishing business continuity policy and objectives;

— implementing and operating controls and measures for managing an organization's overall capability to manage disruptive incidents;

— monitoring and reviewing the performance and effectiveness of the BCMS; and

— continual improvement based on objective measurement.

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

a) a policy;

b) people with defined responsibilities;

c) management processes relating to:

   1) policy;

   2) planning;

   3) implementation and operation;

   4) performance assessment;

   5) management review; and

   6) improvement.

d) a set of documentation providing auditable evidence; and

e) any BCMS processes relevant to the organization.

Business continuity is generally specific to an organization, however, its implementation can have far reaching implications on the wider community and other third parties. An organization is likely to have external organizations that it depends upon and there will be others that depend on it. Effective business continuity therefore contributes to a more resilient society.

The Plan-Do-Check-Act cycle

This International Standard applies the 'Plan-Do-Check-Act' (PDCA) cycle to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organization's BCMS.

Figure 1 illustrates how the BCMS takes interested parties' requirements as inputs for business continuity management (BCM) and, through the required actions and processes, produces business continuity outcomes (i.e. managed business continuity) that meet those requirements.

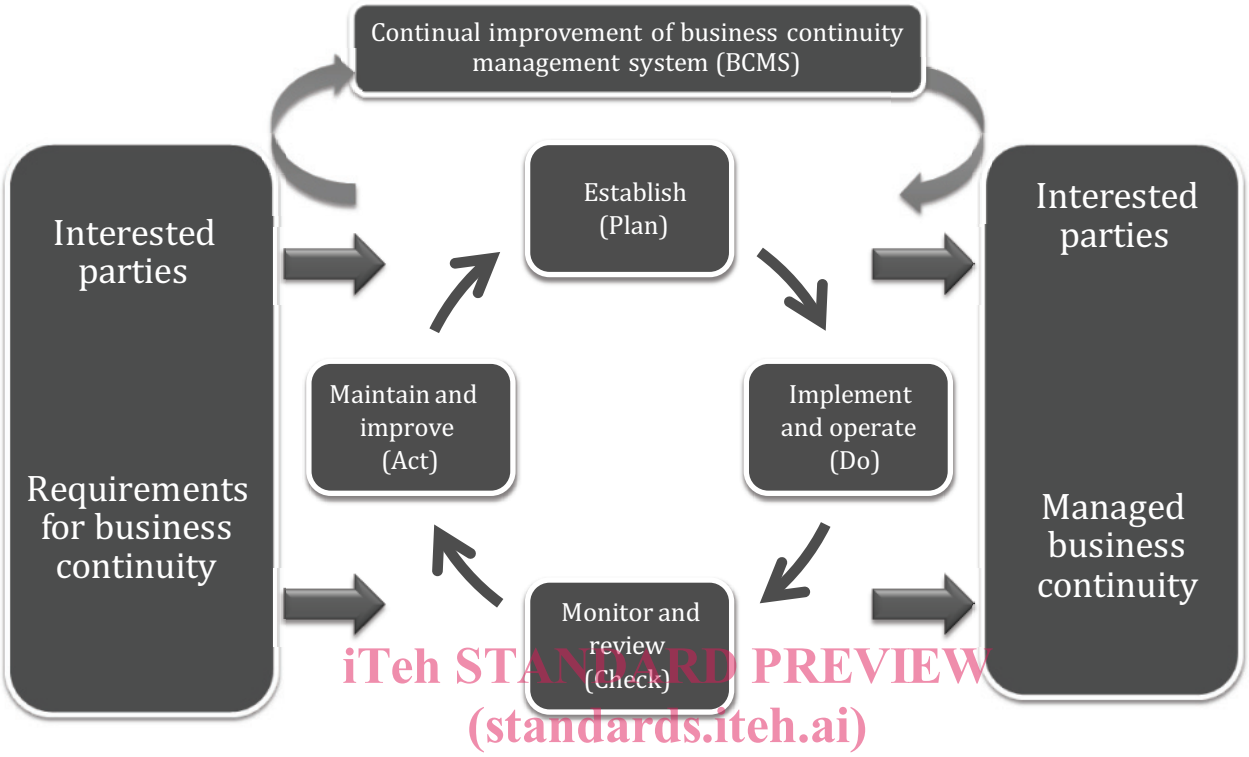

Figure 1 — PDCA model applied to BCMS processes

Table 1 — Explanation of PDCA model

Plan (Establish)	Establish business continuity policy, objectives, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organization's overall policies and objectives.
Do (Implement and operate)	Implement and operate the business continuity policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against business continuity objectives and policy, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the BCMS by taking corrective actions, based on the results of management review and re-appraising the scope of the BCMS and business continuity policy and objectives.

Components of PDCA in this International Standard

There is a direct relationship between the content of Figure 1 and the clauses of this International Standard:

Table 2 — Relationship between PDCA model and Clauses 4 to 10

PDCA component	Clause addressing PDCA component
Plan (Establish)	**Clause 4 (Context of the organization)** sets out what the organization has to do in order to make sure that the BCMS meets its requirements, taking into account all relevant external and internal factors, including:
	— The needs and expectations of interested parties.
	— Its legal and regulatory obligations.
	— The required scope of the BCMS.
	Clause 5 (Leadership) sets out the key role of management in terms of demonstrating commitment, defining policy and establishing roles, responsibilities and authorities.
	Clause 6 (Planning) describes the actions required to establish strategic objectives and guiding principles for the BCMS as a whole. These set the context for the business impact analysis and risk assessment (8.2) and business continuity strategy (8.3).
	Clause 7 (Support) identifies the key elements that need to be in place to support the BCMS, namely: resources, competence, awareness, communication and documented information.
Do (Implement and operate)	**Clause 8 (Operation)** identifies the elements of business continuity management (BCM) that are needed to achieve business continuity.
Check (Monitor and review)	**Clause 9 (Performance evaluation)** provides the basis for improvement of the BCMS through measurement and evaluation of its performance.
Act (Maintain and improve)	**Clause 10 (Improvement)** covers the corrective action needed to address nonconformity identified through performance evaluation.

Business continuity

Business continuity is the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident. Business continuity management (BCM) is the process of achieving business continuity and is about preparing an organization to deal with disruptive incidents that might otherwise prevent it from achieving its objectives.

Placing BCM within the framework and disciplines of a management system creates a business continuity management system (BCMS) that enables BCM to be controlled, evaluated and continually improved.

In this International Standard, the word business is used as an all-embracing term for the operations and services performed by an organization in pursuit of its objectives, goals or mission. As such it is equally applicable to large, medium and small organizations operating in industrial, commercial, public and not-for-profit sectors.

Any incident, large or small, natural, accidental or deliberate has the potential to cause major disruption to the organization's operations and its ability to deliver products and services. However, implementing business continuity before a disruptive incident occurs, rather than waiting for this to happen will enable the organization to resume operations before unacceptable levels of impact arise.

BCM involves:

a) being clear on the organization's key products and services and the activities that deliver them;

b) knowing the priorities for resuming activities and the resources they require;

c) having a clear understanding of the threats to these activities, including their dependencies, and knowing the impacts of not resuming them;

d) having tried and trusted arrangements in place to resume these activities following a disruptive incident; and

e) making sure that these arrangements are routinely reviewed and updated so that they will be effective in all circumstances.

Business continuity can be effective in dealing with both sudden disruptive incidents (e.g. explosions) and gradual ones (e.g. flu pandemics).

Activities are disrupted by a wide variety of incidents, many of which are difficult to predict or analyse. By focusing on the impact of disruption rather than the cause, business continuity identifies those activities on which the organization depends for its survival, and enables the organization to determine what is required to continue to meet its obligations. Through business continuity, an organization can recognize what needs to be done to protect its resources (e.g. people, premises, technology and information), supply chain, interested parties and reputation, before a disruptive incident occurs. With that recognition, the organization is able to take a realistic view on the responses that are likely to be needed as and when a disruption occurs, so that it can be confident of managing the consequences and avoid unacceptable impacts.

An organization with appropriate business continuity in place can also take advantage of opportunities that might otherwise be judged to be too high risk.

The following diagrams (Figures 2 and 3) are intended to illustrate conceptually how business continuity can be effective in mitigating impacts in certain situations. No particular timescales are implied by the relative distance between the stages depicted in either diagram.

Mitigating impacts through effective business continuity – sudden disruption

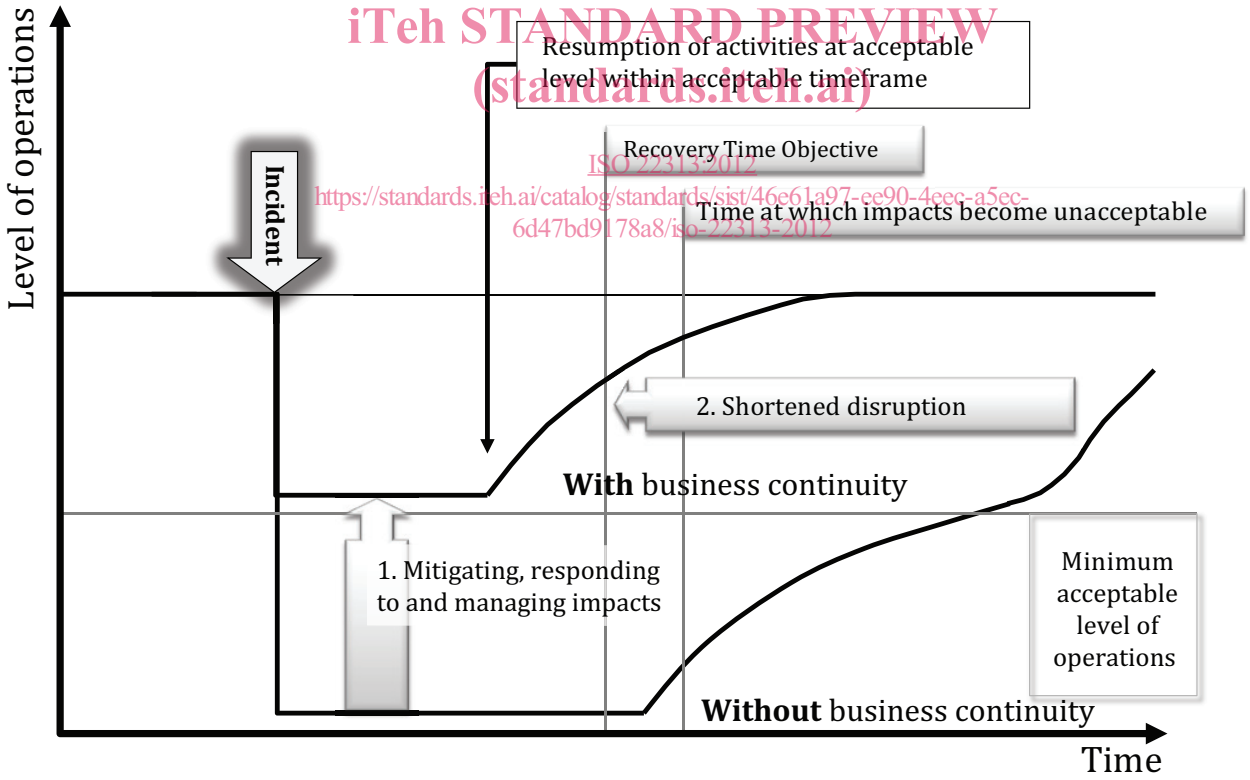

Figure 2 — Illustration of business continuity being effective for sudden disruption

Mitigating impacts through effective business continuity – gradual disruption

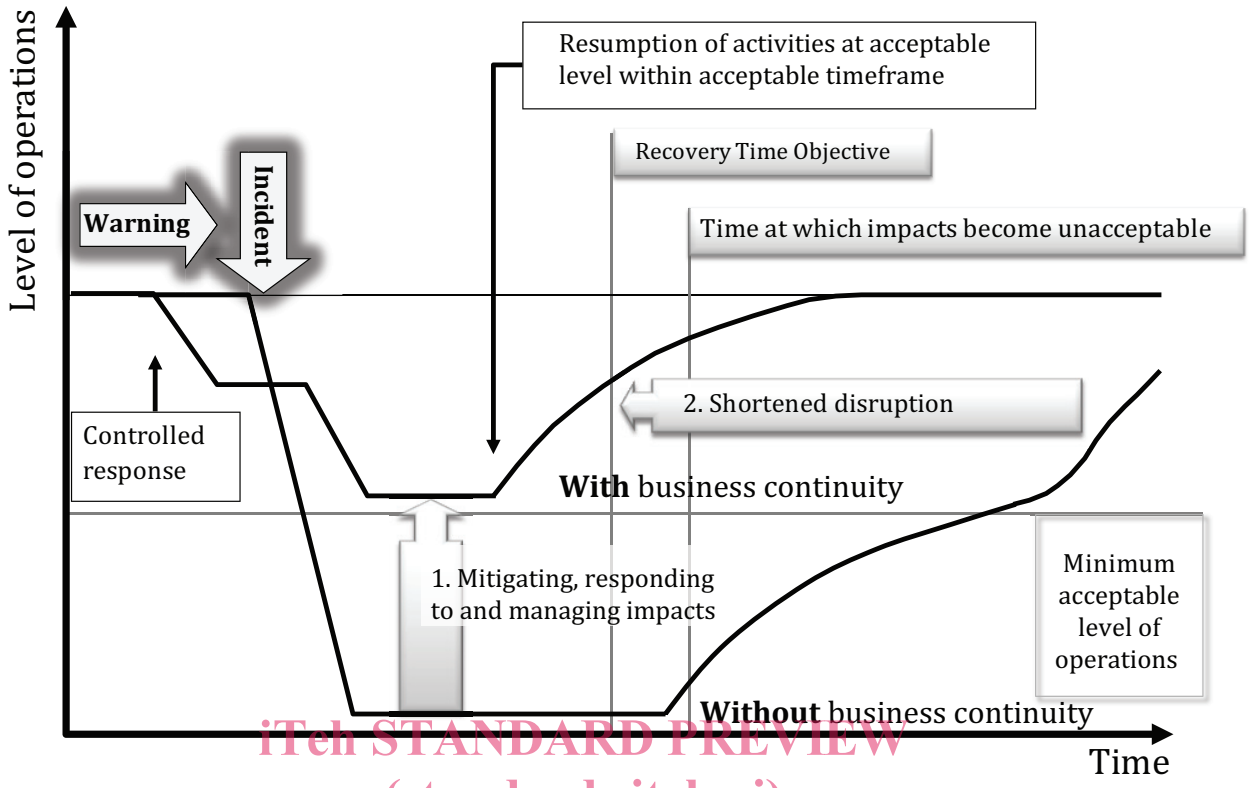

Figure 3 — Illustration of business continuity being effective for gradual disruption (e.g. approaching pandemic)

Societal security — Business continuity management systems — Guidance

1 Scope

This International Standard for business continuity management systems provides guidance based on good international practice for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving a documented management system that enables organizations to prepare for, respond to and recover from disruptive incidents when they arise.

It is not the intent of this International Standard to imply uniformity in the structure of a BCMS but for an organization to design a BCMS that is appropriate to its needs and that meets the requirements of its interested parties. These needs are shaped by legal, regulatory, organizational and industry requirements, the products and services, the processes employed, the environment in which it operates, the size and structure of the organization and the requirements of its interested parties.

This International Standard is generic and applicable to all sizes and types of organizations, including large, medium and small organizations operating in industrial, commercial, public and not-for-profit sectors that wish to:

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

b) ensure conformance with the organization's business continuity policy; or

c) make a self-determination and self-declaration of compliance with this International Standard.

This International Standard cannot be used to assess an organization's ability to meet its own business continuity needs, nor any customer, legal or regulatory needs. Organizations wishing to do so can use the ISO 22301 requirements to demonstrate conformance to others or seek certification of its BCMS by an accredited third party certification body.

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 document (including any amendments) applies.

ISO 22300, *Societal security — Terminology*

ISO 22301, *Societal security — Business continuity management systems — Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and ISO 22301 apply.

4 Context of the organization

4.1 Understanding of the organization and its context

This section is about understanding the context of the organization in relation to setting up and managing the BCMS. The setting up and management of BCM is covered in 8.1.

The organization should evaluate and understand the internal and external factors that are relevant to its purpose and operations. This information should be taken into account when establishing, implementing, maintaining and improving the organization's BCMS, and assigning priorities.

Evaluating the organization's external context should include, where relevant, the following factors:

— the political, legal and regulatory environment whether international, national, regional or local;

— the social and cultural, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

— supply chain commitments and relationships;

— consideration of internal studies on the risks, taking into account other relevant information management systems and more generally any information from knowledge management;

— key drivers and trends having impact on the objectives and operation of the organization; and

— relationships with, and perceptions and values of, interested parties outside the organization.

Evaluating the organization's internal context should include, where relevant, the following factors:

— products and services, activities, resources, supply chains, and relationships with interested parties;

— the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);

— information systems, information flows, and decision making processes (both formal and informal);

— interested parties within the organization;

— policies and objectives, and the strategies that are in place to achieve them;

— future opportunities and business priorities;

— perceptions, values and culture;

— standards and reference models adopted by the organization; and

— structures (e.g. governance, roles and accountabilities).

4.2 Understanding the needs and expectations of interested parties

4.2.1 General

When establishing its BCMS, the organization should ensure that the needs and requirements of interested parties are taken into consideration.

The organization should identify all interested parties that are of relevance to its BCMS and based on their needs and expectations, determine their requirements. It is important to identify not only obligatory and stated requirements but also any that are implied.

NOTE The organization needs to be aware of all those who have an interest in the organization, such as the media, the public nearby, competitors and so on.

When planning and implementing the BCMS, it is important to identify actions that are appropriate in relation to interested parties but differentiate between the different categories. For example, while it may be appropriate to communicate with all interested parties following a disruptive incident, it may not be appropriate to communicate with all interested parties when setting up and managing BCM (8.1.1).

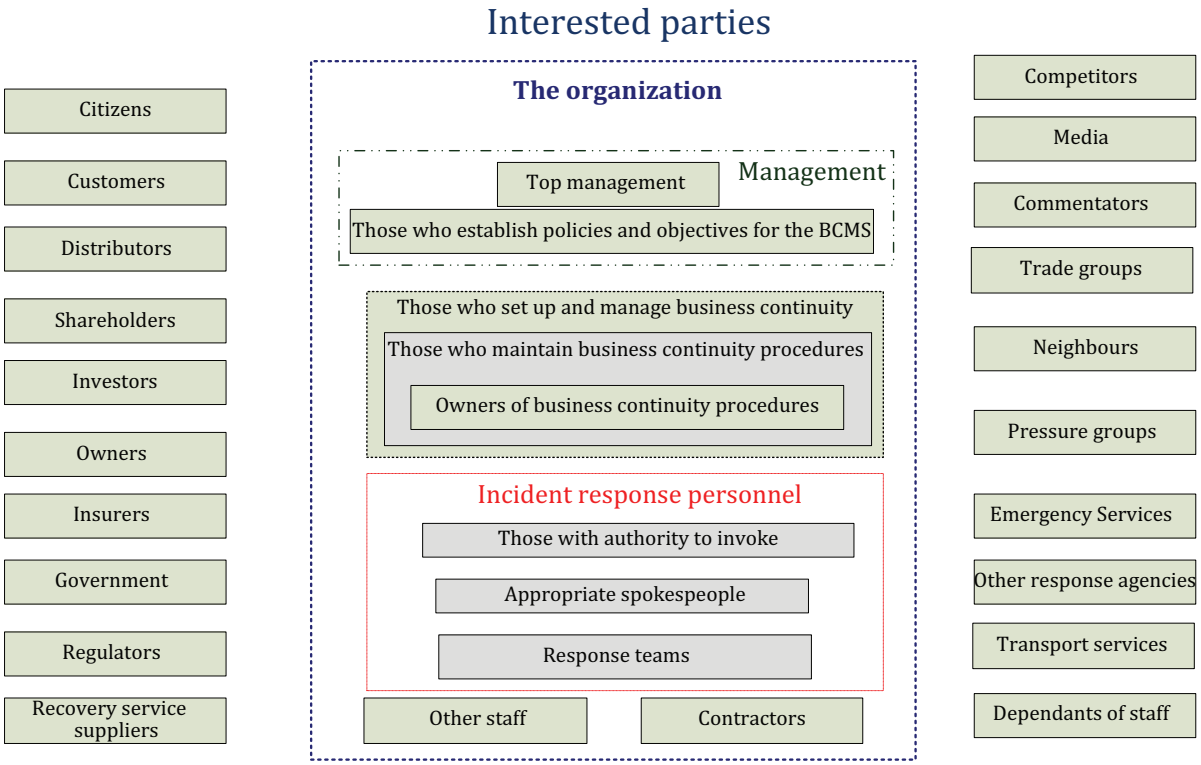

Figure 4 — Examples of interested parties to be considered in public and private sectors

4.2.2 Legal and regulatory requirements

All management systems should operate within the framework of the legal and regulatory environment in which the organization operates. The organization should therefore identify and accommodate in its BCMS all relevant and applicable legal and regulatory requirements to which it subscribes and needs of interested parties.

The information regarding these requirements should be documented and kept up-to-date. New or variations to legal, regulatory and other requirements should be communicated to affected employees and other interested parties.

When establishing, implementing and maintaining the BCMS, the organization should take into account and document applicable legal requirements, other requirements to which it subscribes and needs of interested parties.

The organization should ensure that its BCMS works within and in support of its legal obligations and relevant requirements of interested parties.

The organization should review current and pending statutory and regulatory requirements in their locations which may include:

a) incident response: including emergency management and health, safety and welfare legislation;

b) continuity: which may specify the scope of the programme or the extent or speed of response;

c) risk: requirements defining the scope or methods of a risk management programme; and

d) hazards: operating requirements relating to dangerous materials stored at the location.

NOTE Organizations operating in multiple locations often have to satisfy the requirements of different jurisdictions.

4.3 Determining the scope of the management system

4.3.1 General

The organization should determine the scope of the BCMS and ensure that it may be suitably communicated to interested parties. It is important that the boundaries and applicability of the BCMS are clearly apparent and that the scope takes into account the issues identified in Clause 4.1 and Clause 4.2.

The scope determines the products and services, locations, functions, processes and activities to which the BCMS applies. It follows that all dependencies will be in the scope even if they have not been explicitly identified in the scope statement. For example if 'employee remuneration' is specified in the scope, then by default the availability of funds, management approval and instructions to the financial institution to make payment would also be within the scope.

The organization should clearly document the scope and context of the BCMS.

4.3.2 Scope of the BCMS

The organization should, in a manner and in terms appropriate to the size, nature and complexity of the organization, define and document the scope of the BCMS.

The scope should:

a) identify the parts of the organization included in the BCMS;

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

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

d) take into account the needs and interests of interested parties.

The scope may also:

— include an indication of the scale of incident that the BCMS will address and the organization's risk appetite; and

— identify how the BCMS fits into the organization's overall risk management strategy (if present).

Where part of an organization is excluded from the scope of its BCMS, the organization should document and explain the exclusion.

The purpose of defining the scope is to ensure coverage of all relevant activities, locations and suppliers (8.2.1, Figure 6).

4.4 Business continuity management system

This is normative reference to ISO 22301:2012 which specifies the requirements for a BCMS. No guidance is provided.

5 Leadership

5.1 Leadership and commitment

All levels of relevant management throughout the organization should demonstrate commitment and leadership in implementing business continuity policy and objectives. Demonstration may be achieved using motivation, engagement and empowerment.

5.2 Management commitment

Top management should demonstrate its commitment to the BCMS.

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

a) complying with applicable legal requirements and with other requirements to which the organization subscribes (4.2.2);

b) integrating BCMS processes into the organization's established maintenance and review procedures;

c) establishing business continuity policy and objectives in line with the objectives, obligations and strategic direction of the organization (5.3);

d) appointing one or more persons with the appropriate authority and competencies to be responsible for the BCMS and accountable for its effective operation (5.4);

e) ensuring that BCMS roles, responsibilities and competencies are established (5.4);

f) ensuring the availability of sufficient resources, including appropriate levels of funding (7.1);

g) communicating to the organization the importance of fulfilling business continuity policy and objectives (7.4);

h) actively engaging in exercising and testing (8.5);

i) ensuring that internal BCMS audits are conducted (9.2);

j) conducting effective management reviews of the BCMS (9.3); and

k) directing and supporting improvement of the BCMS (Clause 10).

Management commitment may also be demonstrated by:

— operational involvement through steering groups;

— inclusion of business continuity as a standing item at management meetings.

5.3 Policy

Top management should define the business continuity policy in terms of the organization's objectives and its obligations and make sure that it:

— is appropriate to the purpose of the organization (given its size, nature and complexity and in order to reflect its culture, dependencies and operating environment);

— provides a framework for objective setting;

— includes clear commitments in relation to applicable requirements, including legal and regulatory obligations and continual improvement of the BCMS;

— is communicated and understood within the organization;

— is complementary to other relevant policies; and

— is made available to interested parties as approved by management.

Suitable provisions should be made for approving the policy, retaining documented information on it and reviewing it periodically (for example annually), and whenever significant changes to internal or external factors occur (for example change in top management or introduction of new legislation). The suitability of such provisions will depend on the size, complexity, nature and extent of the organization.