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)

COPYRIGHT PROTECTED DOCUMENT

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.

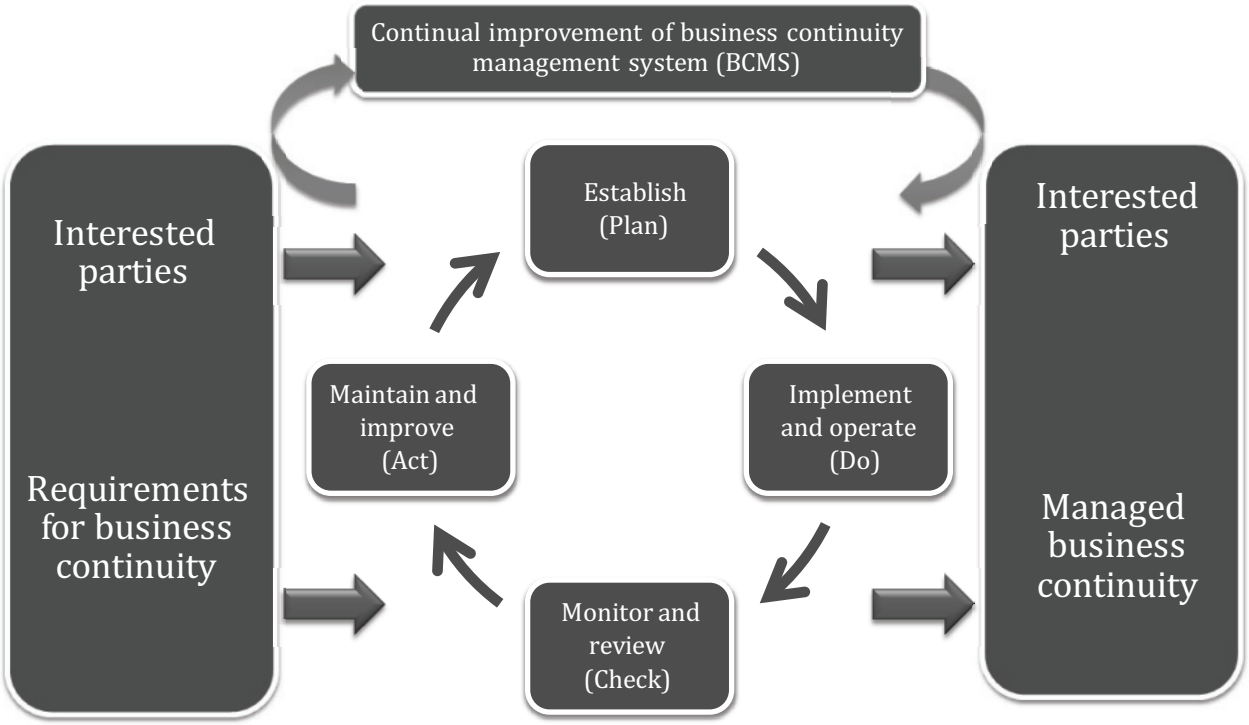

Figure 1 — PDCA model applied to BCMS processes

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

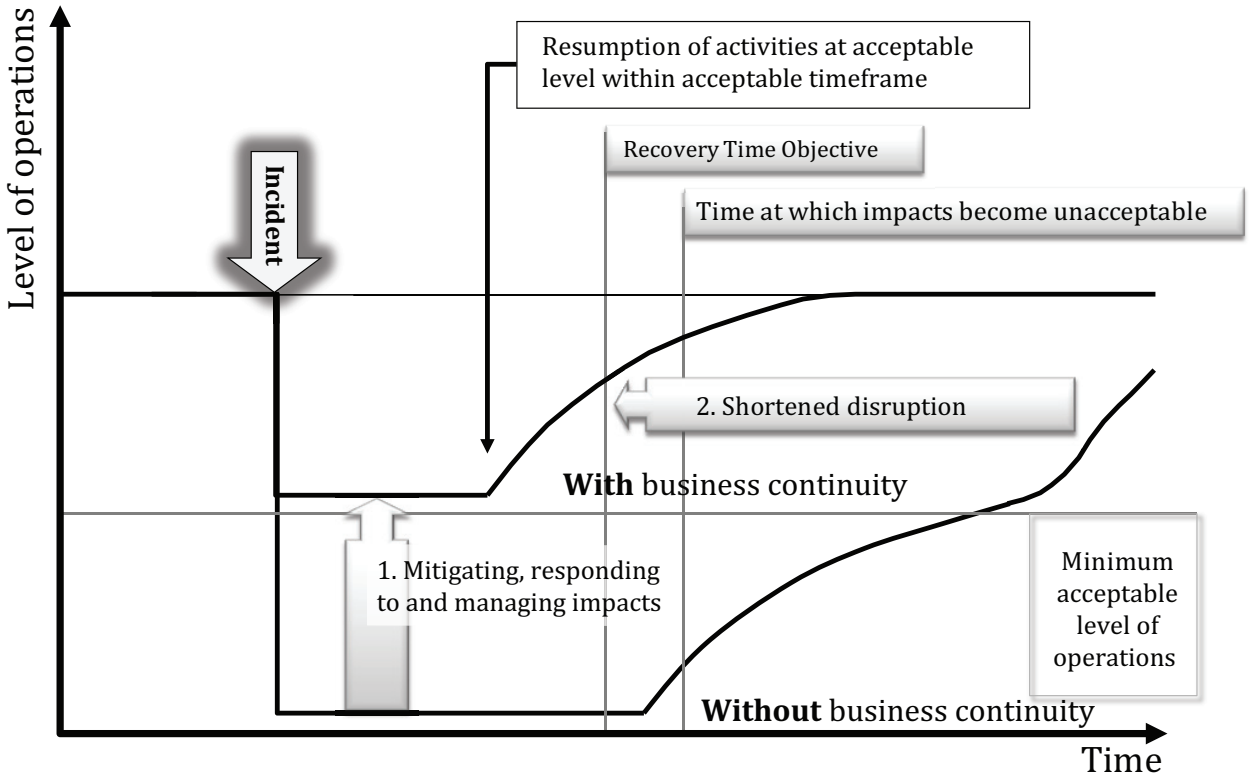

Figure 2 — Illustration of business continuity being effective for sudden disruption

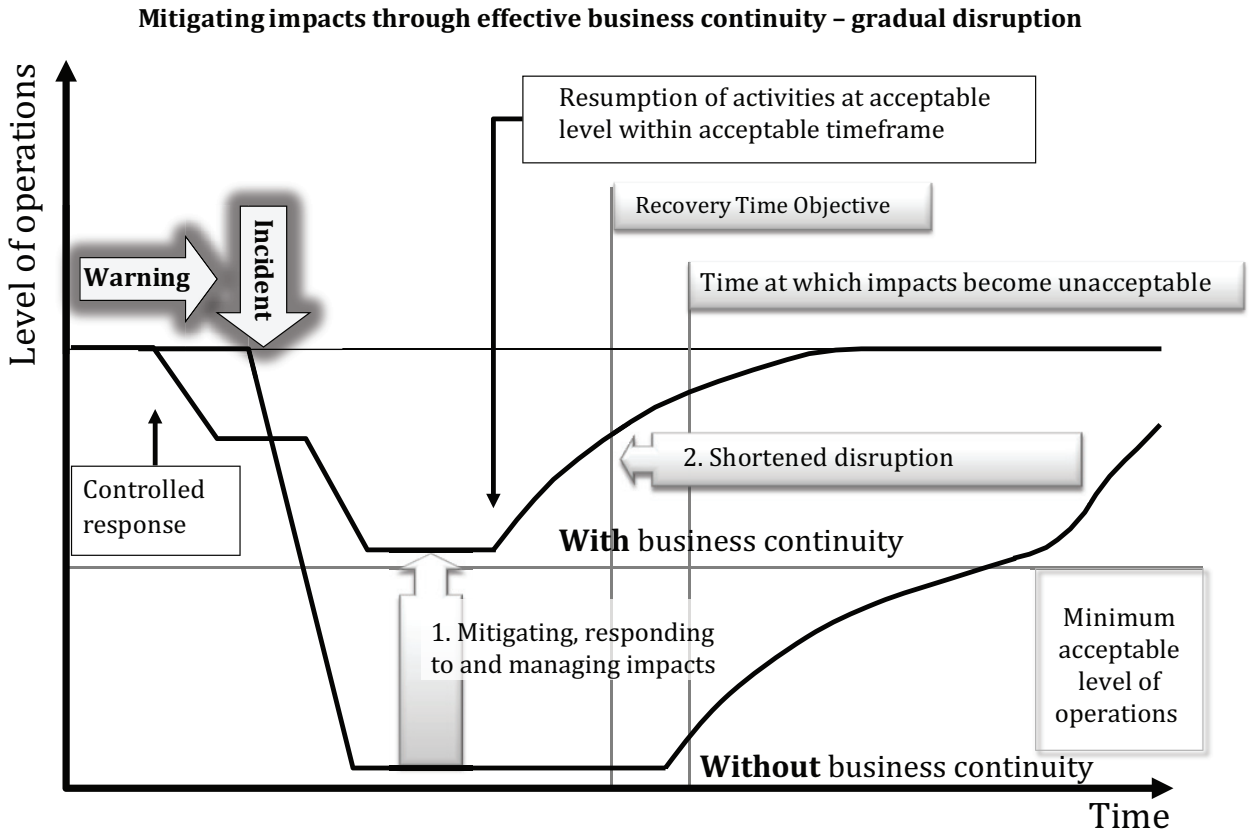

Figure 3 — Illustration of business continuity being effective for gradual disruption (e.g. approaching pandemic)

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).

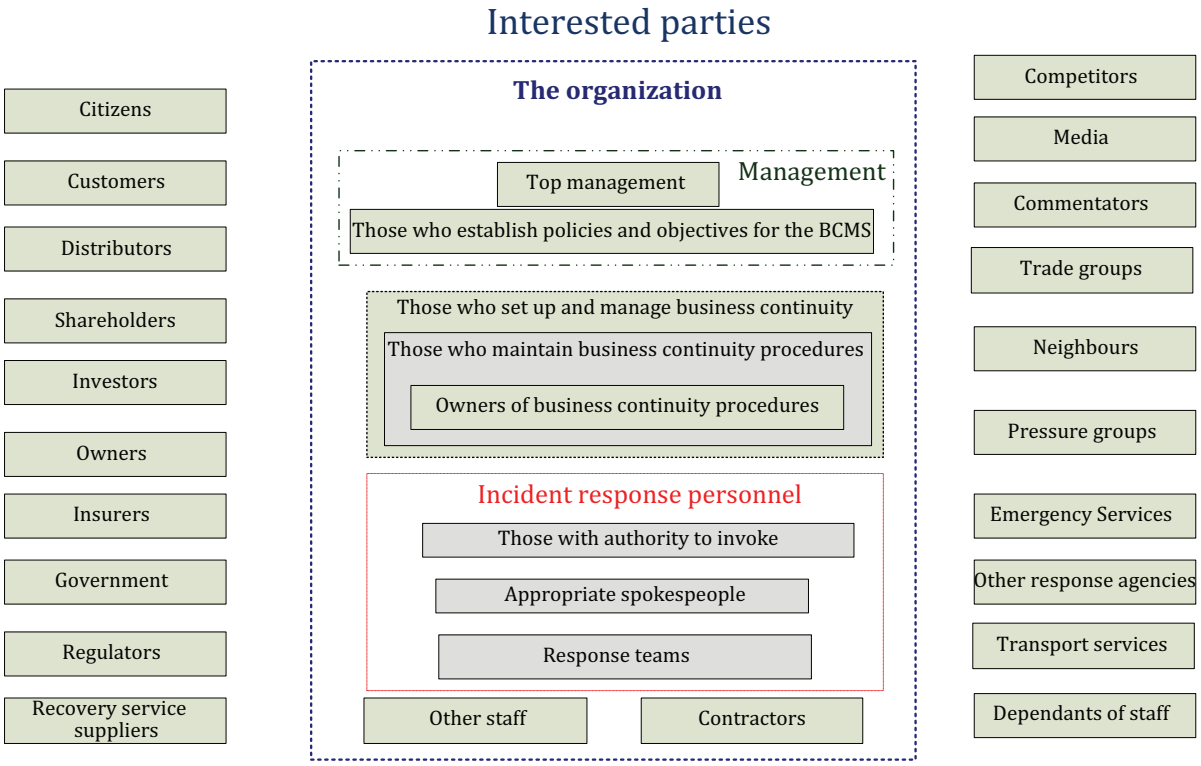

Figure 4 — Examples of interested parties to be considered in public and private sectors

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.

The policy should also:

— provide direction on scope and boundaries of the organization's business continuity including limitations and exclusions;

— identify any authorities and delegations required, including person or persons responsible for the organization's BCMS;

— establish the criteria for type and scale of incidents to be addressed; and

— include references to standards, guidelines, regulations or policies that the BCMS should consider or comply with.

The business continuity policy may contain the following:

— key terms;

— funding commitment;

— references to other related policies;

— a requirement to implement business continuity;

— a commitment to exercise and maintain business continuity.

5.4 Organizational roles, responsibilities and authorities

Top management should ensure the assignment and communication of responsibilities and authorities within the BCMS.

A member of top management should have overall responsibility and accountability for the BCMS.

The organization's top management should appoint one or more specific management representatives who, irrespective of other responsibilities, should have defined roles, responsibilities and authority for:

— ensuring that BCM is established, implemented and maintained in accordance with the business continuity policy;

— reporting on the performance of BCM to top management for review and as the basis for improvement;

— promoting awareness of business continuity throughout the organization; and

— ensuring the effectiveness of procedures developed for incident response, but not necessarily in their implementation during an incident.

The management representative may:

— be known as the 'business continuity manager';

— hold other responsibilities within the organization; and

— reside in many areas of an organization depending on its size, scale and complexity.

Representatives from each function or location of the organization may be identified to assist in the implementation of the BCMS. Their roles, accountabilities, responsibilities and authorities should be integrated into job descriptions which may be reinforced by including them in the organization's appraisal, reward and recognition policy.

Top management may appoint other bodies, for example, a steering committee, to oversee the implementation and on-going monitoring of BCM.

All roles, responsibilities and authorities for BCM should be defined and documented and be subject to audit.

6 Planning

6.1 Actions to address risks and opportunities

The organization should determine how any issues identified in 4.1 and requirements in 4.2 will be addressed.

This should involve evaluating the need for a plan of action to:

— prevent unintended outcomes;

— take advantage of any opportunities to improve the BCMS.

If necessary it should also involve:

— integrating and implementing these actions into the BCMS process (8.1); and

— ensuring that documented information will be available to evaluate if the actions have been effective (7.5).

6.2 Business continuity objectives and plans to achieve them

A plan for setting up and managing BCM (as set out in Clause 8) should be drawn up and should include identifying responsibilities and setting appropriate and realistic targets for the completion of tasks. The plan should be based on continuity objectives that have been set and communicated to relevant functions and levels within the organization. Progress on the plan should be monitored and documented.

This plan should be reviewed and may need to be updated regularly as the BCMS evolves.

The following are examples of business continuity objectives that may, in certain circumstances, meet the requirements specified in ISO 22301:

— 'to set up a BCMS that is consistent with ISO 22313 by *date*';

— 'to achieve certification against ISO 22301:2012 by *date*';

— 'by *date*, we will have business continuity in place that meets our obligations to key customers'; and

— 'to have BCM in place that protects key products and services by *date*'.

7 Support

7.1 Resources

7.1.1 General

The organization should determine and provide the resources needed for the BCMS that will:

a) achieve its business continuity policy and objectives;

b) meet the changing requirements of the organization;

c) enable effective communication on business continuity management system matters, internally and externally; and

d) provide for the on-going operation and continual improvement of the business continuity management system.

These should be provided in a timely and efficient manner.

7.1.2 BCMS resources

When identifying the resources required for the BCMS, the organization should make adequate provision for:

a) people and people-related resources, including:

   1) the time necessary to fulfil BCMS roles and responsibilities;

   2) training, education, awareness and exercising;

   3) management of BCMS personnel;

b) facilities, including appropriate work locations and infrastructure;

c) information and communications technology (ICT), including applications that support effective and efficient programme management;

d) management and control of all forms of documented information;

e) communication with interested parties (see Figure 4); and

f) finance and funding.

Resources and their allocation should be reviewed periodically in order to ensure their adequacy. It may be appropriate to involve top management in this review.

7.1.3 Incident response personnel

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

The incident response personnel should form a group that is responsible for managing any disruptive incident that significantly impacts or has the potential to significantly impact the organization.

Personnel may be assigned to teams according to their demonstrated competence of dealing with different aspects of incident response, for example:

— Incident management/ strategic management (8.4.4.3.1);

— Communications (8.4.4.3.2);

— Safety and welfare (8.4.4.3.3);

— Salvage and security (8.4.4.3.4);

— Resuming activities (8.4.4.3.5);

— Recovery of ICT (8.4.4.3.6).

All personnel who are in these groups should have clearly defined responsibilities and authorities that apply before, during and after an incident.

7.2 Competence

The organization should establish an appropriate and effective system for managing competence of persons undertaking BCMS work under its control.

Management should determine the competences required for all BCMS roles and responsibilities and the awareness, knowledge, understanding, skills and experience needed to fulfil them. All persons assigned roles within the organization should demonstrate the competencies required and be provided

with training, education, development and other support needed to do so. This may be referred to as a competence development programme that may include:

— assessment of competences for role(s) to be undertaken;

— creation of a personal development programme that identifies training, education, development and other support needed to attain competences;

— provision of training and mentoring including selection of suitable methods and materials;

— knowledge sharing;

— job sharing;

— hiring or contracting competent persons;

— training of target groups;

— documentation and monitoring of training received;

— evaluation of training received against defined training needs and requirements in order to verify conformity with BCMS training requirements; and

— improvement of development programme as needed.

The organization should have a process for identifying and delivering the business continuity training requirements of all participants and evaluating the effectiveness of its delivery.

The type of training that may be appropriate for specific roles are as follows:

a) setting up and managing the BCMS:

   1) set up and management of BCM;

   2) conducting a business impact analysis;

   3) risk assessment;

   4) communications skills;

   5) developing and implementing business continuity documentation; and

   6) running an exercise programme.

b) incident response and business recovery:

   1) incident assessment;

   2) evacuation and shelter in place management, including check-in processes to account for employees;

   3) arrangements at alternate worksites; and

   4) handling of media enquiries.

Response skills and competence throughout the organization should be developed by practical training, including active participation in exercises.

Response and recovery teams should receive education and training about their responsibilities and duties including interactions with first responders and other interested parties. Teams should be trained at regular intervals (at least annually), and new members should be trained when they join the response structure. These teams should also receive training on prevention of incidents that may escalate into crises.

Changes in the business environment and operations affect the approach and manner in which business continuity activities are planned, designed and implemented. The organization may demonstrate awareness of BCM trends by, for example, actively participating in industry BCM activities which may include:

— membership of an industry interest group;

— membership of a conference organizing committee;

— delivering presentations at conferences and seminars; and

— attendance at local or global BCM conferences.

Demonstration of active participation may be in one or more of the following ways:

— membership of organizing committee of conferences and seminars; and

— presentation of paper at conferences and seminars.

Competence may be reinforced by any of the following:

— integration of BCMS achievements into the organization's reward and recognition process;

— integration of BCMS achievements into the organization's performance and appraisal process;

— integration of BCMS roles, accountabilities, responsibilities and authority within the organization's job descriptions and skills set; and

— active participation by business users and top management in rehearsals, exercises and tests.

The organization should establish training and awareness programmes for all current employees who may be affected by a disruptive incident and require contractors working on its behalf to demonstrate that person(s) doing work under its control have the requisite competence for the BCMS and response roles that they will perform.

7.3 Awareness

Persons working under the organization's control should have appropriate awareness of the BCMS.

Such persons may include staff, contractors, suppliers. They should be aware of the business continuity policy and:

— their role and responsibility with regard to incident prevention, detection, mitigation, self-protection, evacuation, response, continuity and recovery;

— the importance of conformity with business continuity policy and procedures;

— the implications of changes in the operation of the organization;

— their contribution to the effectiveness of the BCMS, including the benefits of improved BCM performance; and

— their role and responsibility in achieving conformity with its requirements.

The organization should build, promote and embed a culture within the organization that:

— becomes part of the organization's core values and management; and

— makes interested parties aware of the business continuity policy and their role in associated procedures.

An organization with a positive business continuity culture will:

— develop business continuity more efficiently;

— instil confidence in its interested parties (especially staff and customers) in its ability to handle disruptive incidents;

— increase its resilience over time by ensuring business continuity implications are considered in decisions at all levels; and

— minimize the likelihood and impact of disruptions.

Development of a BC culture is supported by:

— involvement of all personnel in the organization;

— dispersed leadership across the organization;

— assignment of responsibilities;

— measurement based on performance indicators;

— integrating business continuity into normal management practices;

— awareness raising;

— skills training; and

— exercising business continuity plans.

An awareness programme may include:

— a consultation process with staff throughout the organization concerning the set up and management of BCM;

— discussion of business continuity in the organization's newsletters, briefings, introduction programme or journals (including new employee orientation);

— inclusion of business continuity on relevant web pages;

— inclusion of BCM as a topic in staff and management team meetings;

— selective publication of post incident reports following incidents;

— briefings for top management;

— visits to designated alternative location (e.g. a recovery site); and

— briefing key suppliers and distributors on the organization's business continuity arrangements.

7.4 Communication

When setting up and managing the BCMS, the organization should have effective communication and consultation procedures for the exchange of information with interested parties.

These should include all of the following:

a) internal communication amongst interested parties, including employees within the organization;

b) external communication with customers, suppliers, local community, and other interested parties, including the media;

c) receiving, documenting, and responding to communication from all interested parties;

d) adapting and integrating a national or regional threat advisory system or equivalent into planning and operational use, where and if appropriate;

e) ensuring availability of the means of communication during a disruptive incident;

f) ensuring the capability of the organization to communicate with external authorities and where appropriate, ensuring that other organizations and personnel are able to communicate amongst themselves; and

g) operating and testing of communications capabilities intended for use during disruption of normal communications.

The organization may invite any external resources that may be involved in a response – such as Fire, Police, Public Health and third party vendors – to review with management relevant parts of its business continuity procedures.

The organization may include references to its BCMS and business continuity arrangements in supplier and customer newsletters and briefings.

The organization should provide effective external communication as part of its awareness programme (7.3) and following an incident (8.4).

7.5 Documented information

7.5.1 General

Documented information provides evidence of conformity to requirements and effective operation of the management system.

The term 'procedure' means a specified way to carry out an activity or a process. A 'documented procedure' means that the procedure should be established and maintained on any medium.

A single document may address the requirements for one or more documented procedures and a requirement for a documented procedure may be covered by more than one document.

Documented information required by this International Standard includes:

— The context of the organization (4.1);

— Legal, regulatory and other requirements and evidence of compliance (4.2.2);

— Scope of the BCMS and any exclusions (4.3.2);

— Business continuity policy (5.3);

— Business continuity objectives (6.2);

— Competence (7.2);

— Business impact analysis and risk assessment process (8.2);

— Business continuity strategy (8.3) including strategy options considered;

— Continuity, incident management and recovery procedures (8.4);

— Post-exercise reports (8.5);

— BCMS monitoring (9.1);

— Internal audits (9.2);

— Management reviews (9.3);

— Nonconformity and corrective action (10.1).

In addition, documented information covering the following information may be required to ensure the effectiveness of the BCMS:

— customer contracts and service levels;

— results of business impact analyses;

— results of risk assessments;

— determination and selection of business continuity strategies;

— incident response overview;

— awareness programme;

— BCMS and incident communications with staff and interested parties - such as newsletters, meeting notes and alerts;

— training programmes for the organization and individuals;

— exercise schedule;

— contracts and service level agreements with suppliers;

— contractor and supplier notification and response procedures;

— evidence of inspection, maintenance and calibration;

— post-incident reports of incidents and near-hits;

— BCMS review meeting minutes.

7.5.2 Create and update

In order to comply with the requirements for creating and updating documented information:

— all documented information should include its identification and description (e.g. a title, name, date, author, number, revision reference etc.;

— acceptable formats should be specified (e.g. language, software version, graphics) and media (e.g. paper, electronic) for the capture and presentation of documented information should be clearly stated;

— all documented information should be reviewed and approved for adequacy.

The capture and presentation should include the format to be used (e.g. language, software version, graphics) and the media to be used (e.g. paper, electronic document).

The extent of documented information for the BCMS may differ between organizations due to the following factors:

— the size of organization, its products and services and the type of activities that it undertakes;

— the complexity of activities and their interactions; and

— the competence of persons.

7.5.3 Control of documented information

All required documented information should be controlled.

The purpose of controlling documentation is to ensure that organizations create, maintain and protect documents in a manner that is appropriate and sufficient to implement and operate the BCMS. The primary focus should be on this purpose rather than establishing a complex document control system.

Examples of protection include preventing documents from being compromised, modified without appropriate authorization and accidentally deleted.

There are various access levels and combinations that may be granted, for example, view only, view and change and restricted view.

A documented procedure should be established to define the controls that are needed to:

a) distribute documented information;

b) provide access to it (access includes, for example, the permissions and authority to view or change documented information);

c) approve documents for adequacy prior to issue;

d) review and update as necessary and re-approve documents;

e) ensure that changes and the current revision status of documents are identified;

f) ensure that relevant versions of applicable documents are available at points of use;

g) ensure that documents remain legible and readily identifiable;

h) ensure that documents of external origin determined by the organization to be necessary for the planning and operation of the BCMS are identified and their distribution controlled;

i) prevent the unintended use of obsolete documents and to apply suitable identification to them if they are retained for any purpose;

j) establish document retention and archival parameters; and

k) ensure the protection and non-disclosure of confidential information.

Organizations should ensure the integrity of documented information by rendering it tamperproof, securely backed-up, accessible only to authorized personnel, and protected from damage, deterioration and loss.

The organization should comply fully with all relevant legislation and regulations regarding the retention of documented information and establish, implement, and maintain the processes required to achieve compliance.

8 Operation

8.1 Operational planning and control

The organization should determine, plan, implement and control those actions needed to fulfil its business continuity policy and objectives and meet applicable needs and requirements.

These actions may be combined to create a programme to ensure that the organization's business continuity is managed appropriately and its effectiveness maintained.

The organization should establish control mechanisms within the programme that include:

a) deciding how these actions should be determined, planned, implemented and controlled, for example by establishing an implementation plan and agreeing a suitable methodology for implementing BCM;

b) ensuring that controls over these actions are implemented in accordance with the decisions made by, for example, setting project milestones and specifying required deliverables; and

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

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

8.1.1 Elements of BCM

BCM comprises the following elements, as illustrated in Figure 5:

Figure 5 — Elements of business continuity management (BCM)

These elements and where they are addressed in this International Standard are as follows:

a) **Operational planning and control** (8.1)

Effective operational planning and control is at the heart of business continuity management. It should be led by a responsible person nominated by top management.

b) **Business impact analysis and risk assessment** (8.2)

Gaining agreement and understanding of priorities and requirements for business continuity is achieved through business impact analysis (BIA) and risk assessment (RA). The BIA enables the organization to prioritize for resumption, the activities that support its products and services. Risk assessment promotes understanding of the risks to prioritized activities and their dependencies and the potential consequences of a disruptive incident. This understanding enables the organization to select appropriate business continuity strategies.

c) **Business continuity strategy** (8.3)

The identification and evaluation of a range of business continuity strategy options enables the organization to choose appropriate ways of preventing disruption of its prioritized activities and dealing with any disruptions that take place. Selected business continuity strategies will provide for the resumption of activities at an acceptable level of operation and within agreed timeframes.

NOTE The chosen strategies need to take into account any risk treatment that is already in place within the organization (8.3.3).

d) **Establish and implement business continuity procedures** (8.4)

Implementing business continuity arrangements results in the creation of an incident response structure (8.4.2), the means for detecting and responding to an incident (8.4.3), business continuity plans (8.4.4) and procedures for returning to 'business as usual (8.4.5).

e) **Exercising and testing** (8.5)

Exercising and testing provide the opportunity for the organization to:

— promote personnel awareness and competency development;

— ensure that business continuity and business continuity procedures are complete, current and appropriate; and

— identify opportunities to improve its business continuity.

8.1.2 Managing the BCM environment

Effective management of the BCM environment includes:

a) ensuring the continuing relevance of the scope, roles and responsibilities for business continuity;

b) promoting and embedding continuity across the organization and other interested parties, where appropriate;

c) managing costs associated with business continuity;

d) establishing and monitoring change management and succession management regimes within the business continuity management system;

e) arranging or providing appropriate staff training and awareness; and

f) maintaining programme documentation appropriate to the size and complexity of the organization.

Each component of an organization's BCM arrangements, including documentation should be regularly reviewed, exercised and updated. These arrangements should also be reviewed and updated whenever there is a significant change in the organization's operational environment, structure, locations, personnel, processes or technology, or when an exercise or incident highlights deficiencies.

The organization may adopt a recognized project management method to ensure that the BCM programme is effectively managed.

8.1.3 Maintaining business continuity

Maintaining effective business continuity includes:

a) keeping BCM current through good practice;

b) administering the exercise programme;

c) coordinating the regular review and update of business continuity, including reviewing or reworking business impact analyses (BIAs) and risk assessments; and

d) ensuring the maintenance of business continuity procedures appropriate to the needs of response teams.

8.1.4 Measuring effectiveness

Measuring effectiveness needs to address both:

a) monitoring the performance of business continuity; and

b) monitoring and reviewing the business continuity arrangements for outsourced activities and the BCM capabilities of suppliers.

Examples of metrics that may be used for measuring effectiveness include:

— activities and resources are recoverable within their specified recovery time objective and information is of the required currency (recovery point objective);

— the required accommodation and equipment are available at alternate location(s) to enable recovery and resumption of activities;

— the required competences to resume the prioritized activities within the specified recovery time objective have been demonstrated; and

— the required competences to respond to and manage incidents have been demonstrated.

8.1.5 Outcomes

Outcomes indicative of effective BCM may include the following:

a) an incident management capability is enabled and provides an effective response;

b) the organization's understanding of itself and its relationships with other organizations, relevant regulators or government departments, local authorities and the emergency services is properly developed, documented and understood;

c) regular exercising ensures that staff are trained to respond effectively to an incident or disruption;

d) requirements of interested parties are understood and able to be delivered;

e) staff receive adequate support and communications in the event of a disruption;

f) the organization's reputation is protected;

g) the organization remains compliant with its legal and regulatory obligations; and

h) financial controls are maintained throughout an incident.

8.2 Business impact analysis and risk assessment

8.2.1 General

The organization should establish, implement and maintain a formal and documented process for business impact analysis (BIA) and risk assessment. The understanding obtained across the organization from the BIA and risk assessment provides the foundation for effective business continuity.

An organization achieves its purpose by delivering its products and services to customers. It is important therefore to create an understanding of the adverse impact over time that disruption of these products and services (and the associated activities) would have on the objectives and operation of the organization. It is also important to understand the inter-relationships and resource requirements of the activities that support products and services and the threats to them.

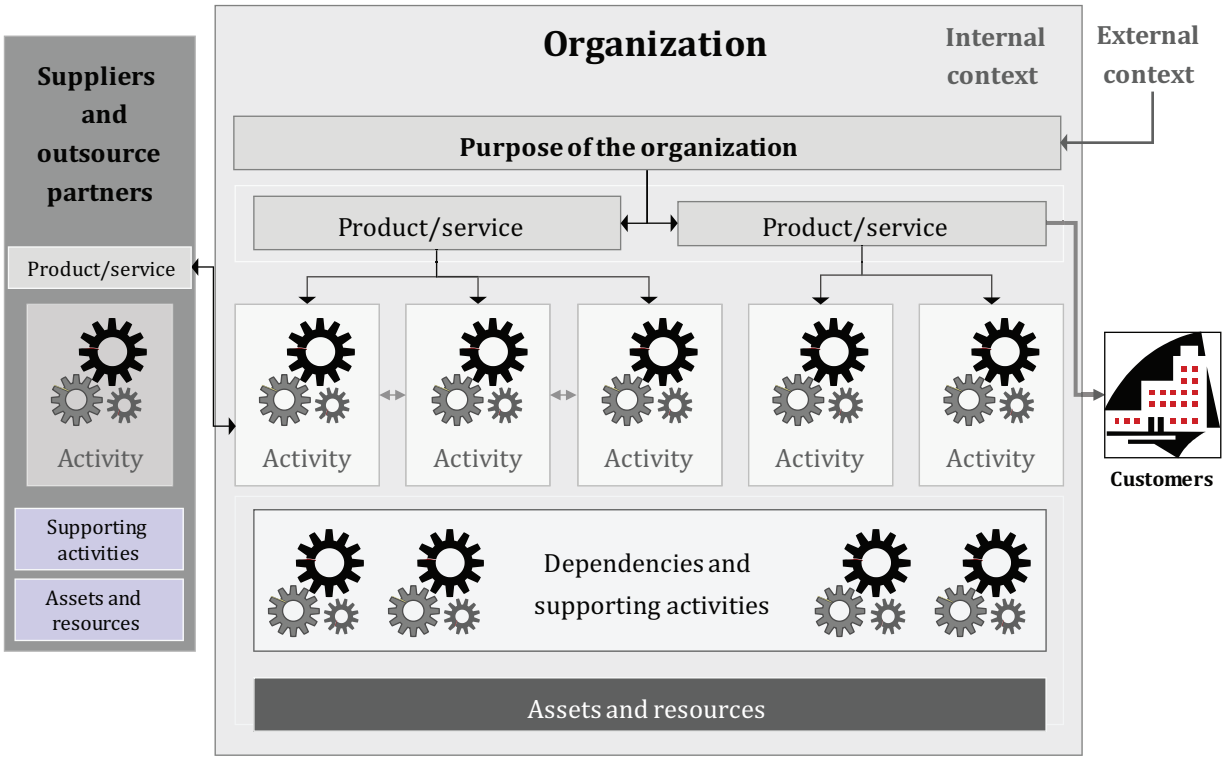

Figure 6 — Understanding the organization

Through understanding, the organization is able to ensure that its business continuity aligns with its purpose, statutory duties and obligations to its interested parties. Understanding is achieved through the processes of business impact analysis and risk assessment. These processes provide the information that the organization needs to determine and select business continuity strategies (8.3.1).

The BIA and risk assessment should enable the organization to identify measures that:

a) limit the impact of a disruption on the organization;

b) shorten the period of disruption; and

c) reduce the likelihood of a disruption.

The context, evaluation criteria and format of the outcome of the BIA and risk assessment should be defined and agreed in advance. Information collected should be regularly reviewed, particularly during periods of change.

8.2.2 Business impact analysis

The organization should establish a formal evaluation process for determining continuity and recovery priorities and objectives.

The purpose of the BIA is to:

— obtain an understanding of the organization's key products and services and the activities that deliver them;

— determine priorities and timeframes for resuming activities;

— identify the key resources likely to be required for continuity and recovery; and

— identify dependencies (both internal and external).

The business impact analysis should include:

a) identifying the activities that support the delivery of the organization's key products and services – 'key' means those included in the scope of the BCMS;

b) assessing the potential impacts over time of disruptions resulting from uncontrolled, non-specific events on these activities. When assessing impacts, the organization should address those relating to its business aims and objectives and its interested parties. These may include:

   1) adverse effects on staff or public well-being;

   2) consequences of breaching statutory duties or regulatory requirements;

   3) damage to reputation;

   4) reduced financial viability;

   5) deterioration of product or service quality; and

   6) environmental damage.

   NOTE 1 Disruption of activities can cause delivery of products and services to be interrupted indirectly. For example the loss of the ability to pay suppliers may damage the reputation of the organization and result in suppliers refusing to supply goods which then prevents products being manufactured or services being delivered.

   NOTE 2 Activities generally have daily variations and can be cyclical in nature. There are often seasonal variations and higher levels of activity associated with weekly, monthly or annual deadlines or project delivery dates. Assuming that the disruption occurs at the worst time during these cycles ensures that the maximum possible impact is assessed.

c) estimating how long it would take for the impacts associated with disruption of the organization's activities to become unacceptable;

   NOTE 3 The time taken for impacts to become unacceptable can vary between seconds and several months depending on the nature of the activity. Activities that are time-sensitive might need to be specified with a great degree of accuracy, e.g. to the minute or the hour. Less accuracy will be acceptable for less time-sensitive activities.

   NOTE 4 The time it would take for impacts to become unacceptable can be referred to as 'maximum tolerable period of disruption', 'maximum tolerable period' or 'maximum acceptable outage'. The minimum level of product or service that is acceptable to the organization can be expressed as the minimum business continuity objective (MBCO).

d) based on the assessment of potential impacts and taking into account other relevant factors, setting prioritized timeframes for resuming these activities, at a specified minimum acceptable level;

e) identifying dependencies between activities; and

f) identifying each activity's dependency on supporting resources, including suppliers and other relevant interested parties.

The prioritized timeframe for resuming an activity may be referred to as Recovery Time Objective (RTO). The RTO may take into account dependencies of interrelated activities and the time within which the impacts of not resuming the activity would become unacceptable [refer to c) above].

NOTE 5 From this point forward in this International Standard, the term 'recovery time objective' or its abbreviation 'RTO' will be used instead of 'prioritized timeframe'.

The output of the business impact analysis should be documented and include identification of:

— products, services and activities;

— recovery priorities;

— significant dependencies and supporting resources.

Information for the business impact analysis may come from:

— interviews;

— questionnaires;

— workshops; and

— other internal and external sources.

8.2.3 Risk assessment

The organization should establish a formal risk assessment process that systematically identifies, analyses and evaluates the risk of disrupting the organization's prioritized activities and the processes, systems, information, people, assets, suppliers and other resources that support them.

Risk assessment provides a structured process for analysing risk in terms of consequences and likelihood before deciding on further treatment that may be required. This structured process attempts to answer some fundamental questions:

a) What may happen and why (risk identification)?

b) What might be the consequences?

c) What is the likelihood of them happening? and

d) Is there anything that might mitigate the consequences or reduce the likelihood?

The process needs to take into consideration financial, governmental and societal obligations.

The organization should understand the threats to and vulnerabilities of the resources required by the organization's activities, and in particular those:

— required by an activity with high priority; or

— with a significant replacement lead-time.

The organization should select an appropriate method for identifying, analysing and evaluating risks that could result in disruptions. ISO 31000 sets out the principles of risk management and associated guidelines. Typical elements that should be included in the context of this International Standard are as follows:

— **identification of risks**: Identify the risks of disruption to the organization's prioritized activities and the processes, systems, information, people, assets, suppliers and other resources that support them. These may come from:

  — specific threats, which may be described as events or actions that could at some point disrupt activities and resources (e.g. threats such as fire, flood, power failure, staff loss, staff absenteeism, computer viruses and hardware failure); and

  — disruptive incidents, which may arise from vulnerabilities within resources (e.g. single points of failure, inadequacies in fire protection, lack of electrical resilience, inadequate staffing levels and poor IT security and resilience);

— **evaluation of risks**: Evaluate which disruption related risks require treatment. This should focus on the resources required by activities with high priority or with significant replacement lead time; and

— **identification of treatments**: Identify treatments that can deliver the business continuity objectives and are in accordance with the organization's risk appetite (4.1).

NOTE If any other analysis of risk has been undertaken by the organization or external bodies, it could provide useful information that is of relevance to the risk assessment.

Societal needs or regulatory obligations may require the organization to share some of the outcomes of the risk assessment with some interested parties.

8.3 Business continuity strategy

8.3.1 Determination and selection

8.3.1.1 General

Determining business continuity strategy is about identifying the action needed to address the findings from the BIA and risk assessment and in a way that meets the business continuity objectives of the organization. Such action is likely to be needed before, during and after a disruptive incident and may, for example, include:

— splitting a manufacturing production line across two locations;

— installing a power generator; or

— reducing the overall impact of a disruptive incident through business continuity arrangements that shorten the period of interruption and reduce its intensity to acceptable levels.

Determination and selection of business continuity strategy should be based on the outputs from the business impact analysis and risk assessment (8.2).

The organization should determine appropriate strategy options for:

— protecting prioritized activities;

— stabilizing, continuing, resuming and recovering prioritized activities;

— mitigating, responding to and managing impacts.

The organization should have in place a mechanism for the review and approval of recommended solutions.

8.3.1.2 Protecting prioritized activities

The protection of prioritized activities may be targeted at:

— reducing the risk to the activity;

— transferring the activity to a third party (though the responsibility remains with the organization); and

— ceasing or changing the activity if viable alternatives are available.

Options for protecting prioritized activities should be selected according to:

— the perceived vulnerabilities of the activity;

— the cost of the measures compared to the estimated benefits;

— (optionally) the urgency of the activity - since there will be less time to resolve the issue; and

— the overall feasibility and suitability of the option.

Where the organization estimates a threat to be 'extremely unlikely' or the cost of protecting a prioritized activity to be prohibitively expensive, it may choose to accept the risk and re-evaluate it as part of its on-going BCMS performance evaluation (Clause 10).

8.3.1.3 Stabilizing, continuing, resuming and recovering prioritized activities

Stabilizing, continuing, resuming and recovering prioritized activities should also address their dependencies and supporting resources;

Business continuity strategy options may include:

a) **Activity relocation**: The transfer of some or all activities either internally to another part of the organization, or externally to a third party, either independently or through a reciprocal or mutual aid agreement;

b) **Resource relocation or reallocation**: Resources, including staff are transferred to another location or activity within the organization, or externally to a third party;

c) **Alternate processes and spare capacity**: Establishing alternate processes or creating redundancy/spare capacity in processes and/or inventory;

d) **Resource and skills replacement**: Enhancing people capabilities, including multi-skilling of key staff or creating access to additional people capability through outsourcing. Replacement resources are provided by a third party or from stock held remotely by the organization or establishing mutual aid agreements with external organizations and key interested parties to provide temporary access to additional capability; and

e) **Temporary workaround**: Some activities may adopt a different way of working which provides acceptable results for a limited time. It is probable that the workaround will be more time consuming and/or labour-intensive (e.g. a manual operation as opposed to an automated system). For these reasons, workarounds are generally only suitable for short periods of time or deferring a return to normal business.

f) When considering locations at which to resume an activity, business continuity options should include the damaged/affected site(s) and undamaged alternate sites(s).

To ensure that activities can be resumed within their recovery time objectives, recovery time objectives may also be set for their dependencies and supporting resources. Setting of these recovery time objectives may need to take into account:

— the possibility of providing a minimum service for a temporary period until the point when full resumption is required;

— workarounds (such as manual processes) which may defer the need for resuming the dependency of supporting resources;

— backlogs and time needed to recover lost data; and

— the complexity and scale of recovery requirements or the need for specialist equipment with a long lead time.

The organization should evaluate all strategy options to determine if these measures have themselves introduced new risks.

Business continuity strategy options for stabilizing, continuing, resuming or recovering a prioritized activity can often be prohibitively expensive. Where the organization estimates this to be the case, it should either select alternative strategies that are acceptable and meet its business continuity objectives or treat affected products and services as exclusions from the scope of the BCMS in accordance with 4.3.2.

8.3.1.4 Mitigating, responding to and managing impacts

Options to mitigate the impact and duration of an incident may include:

a) **Insurance**: Purchase of insurance may provide some financial recompense for some losses, but will not meet all costs (e.g. uninsured events, brand, reputation, interested parties value, market share and human consequences). A financial settlement alone will not fully protect the organization and

satisfy interested parties' expectations. Insurance cover is more likely to be used in conjunction with one or more other strategies;

b) **Asset restoration**: Contracting the stand-by services of companies that specialize in the cleaning or repair of assets following their damage; and

c) **Reputation management**: Developing an effective warning and communication capability (8.4.3) and establishing effective communications procedures (8.4.4.3.2)

8.3.1.5 Business continuity of suppliers

The organization should ensure that the business continuity of suppliers are evaluated. The organization may wish to concentrate its efforts on suppliers whose failure to deliver would most quickly disrupt prioritized activities. Techniques may include:

— specification of requirements in tenders and contracts;

— periodic audits of supplier plans;

— joint business continuity exercises.

8.3.2 Establishing resource requirements

8.3.2.1 General

The organization should determine the resource requirements to implement the selected strategy options.

The organization should establish:

a) appropriate teams or, for smaller organizations, individuals with appropriate authority to oversee incident preparedness, response and recovery;

b) logistical capabilities and procedures to locate, acquire, store, distribute, maintain, test, and account for services, personnel, resources, materials, and facilities produced or donated to support the BCMS;

c) financial, logistical and administrative procedures to support the business continuity arrangements before, during, and after an incident. Procedures should:

   1) ensure that fiscal decisions may be expedited; and

   2) be in accordance with established authority levels, governance, and accounting principles;

d) resource management objectives for response times, personnel, equipment, training, facilities, funding, insurance, liability control, expert knowledge, materials and the time frames within which each will be needed from organization's resources and from any suppliers; and

e) procedures for interested party assistance, communications, strategic alliances, and mutual aid.

8.3.2.2 People

The organization should identify appropriate measures to maintain and widen the availability of core skills and knowledge in the event that the incident results in the reduction of staff availability. These measures should include employees, contractors and other interested parties who possess extensive specialist skills and knowledge. Techniques to protect or enhance those skills may include:

— list of back up skilled specialists and call up plan;

— multi-skill training of staff and contractors;

— separation of core skills to reduce the impact of an incident including physical separation of staff with core skills at more than one location;

— use of third parties;

— succession planning; and

— documenting processes and other forms of knowledge retention and management.

Procedures that rely on the relocation of staff after an incident may need to take into account:

— transportation of staff to another location;

— staff needs at the alternate site such as:

  — accommodation;

  — catering facilities;

  — personal and family commitments; and

  — training on different equipment;

— challenges posed by home working.

Specialist roles may include:

— security;

— transportation logistics; and

— welfare and emergency.

8.3.2.3 Information and data

Information vital to the organization's operation should be protected and recoverable according to the timeframes identified within the BIA. The storage and recovery of data should be compliant with relevant legislation.

NOTE 1 Further guidance on ensuring the currency of electronic data is given in ISO/IEC 27031. ISO/IEC 27002 provides guidance on ensuring the on-going confidentiality, integrity and availability of data.

Any information required to enable the organization's response and recovery should have appropriate:

— **confidentiality**: for example if the activity is moved to another location;

— **integrity**: that the information is reliable and may be trusted;

— **availability**: that the information is available as quickly as the activity requires it. Information required during the response may be required immediately while other data may not be required for some time after the incident; and

— **currency**: as up to date as required enabling the activity to operate - though data lost due to the incident may need to be recreated.

In all cases, information required by an activity should be appropriately current. This currency may be referred to as the recovery point objective (RPO). Where data are copied, various methods may be used, including electronic or tape backups, microfiche, photocopies and creating dual copies at the time of production.

Information strategies should be documented for the recovery of information that has not yet been copied or backed-up to a safe location.

Information strategies should extend to include:

— physical (hardcopy) formats; and

— virtual (electronic) formats, etc.

NOTE 2 If copied information is stored too near to the original, the disruptive incident might compromise its integrity or prevent access to it. However, a long distance may prevent it from being available when it is needed. It would be appropriate to have written evidence as to how these conflicting concerns have been resolved.

Information referred to in this section may include:

— contact information;

— supplier, interested parties and interested party details;

— legal documents (e.g. contracts, insurance policies, title deeds); and

— other services documents (e.g. contracts and service level agreements).

8.3.2.4 Buildings, work environment and associated utilities

Worksite strategies may vary significantly and a range of options might be available. Different types of incident or threat might require the implementation of different or multiple worksite options. The appropriate tactics will in part be determined by the organization's size, sector and spread of activities, by interested parties, and by geographical base. For example, public authorities will need to maintain a frontline service delivery in their communities whereas some organizations could operate from a different country or continent.

The organization should devise a strategy for reducing the impact of the unavailability of its normal worksite(s). This may include one or more of the following:

a) alternative premises (locations) within the organization, including displacement of other activities;

b) alternative premises provided by other organizations (whether or not these are reciprocal arrangements);

c) emergency control centres;

d) alternative premises provided by third-party specialists;

e) working from home or at remote sites;

f) other agreed suitable premises; and

g) use of an alternative workforce in an established site.

Alternative premises should be carefully selected by taking account of a geographical area which may be affected by the same incident. An incident such as a natural disaster may cause damage in wide areas and affect essential services such as electricity, gas, water and communication. If such a risk is expected, alternative premises should be distant from such a possible affected zone.

If staff are to be moved to alternative premises, these premises ought to be close enough that staff are willing and able to travel there, taking into account any possible difficulties caused by the incident. However, the alternative premises ought not to be so close that they are likely to be affected by the same incident.

The use of alternative premises for continuity purposes ought to be supported by a clear statement as to whether the resources required in the alternative premises are for the exclusive use of the organization. If the alternative premises are shared with other organizations, a plan to mitigate the non-availability of these premises ought to be developed and documented.

In some situations (e.g. a manufacturing line or a call centre), it may be appropriate to move the workload rather than the staff. This may require spare capacity at the alternate site or additional staff (whether by overtime or recruitment) and other resources to be made available.

8.3.2.5 Facilities, equipment and consumables

The organization should identify and maintain an inventory of the core supplies that support its prioritized activities.

Some facilities and machinery may be difficult to acquire, be very expensive (requiring a long time for authorization) or have long lead times. Solutions for providing such resources may need to take such issues into account. Changing business practices, such as stock control or building management may provide solutions.

Techniques for providing these may include:

— storage of additional supplies at another location;

— arrangements with third parties for delivery of stock at short notice;

— diversion of just-in-time deliveries to other locations;

— holding of materials at warehouses or shipping sites;

— transfer of sub-assembly operations to an alternative location which has supplies;

— identification of alternative/substitute supplies; and

— identification of facilities and equipment and multi-option planning by phases.

Where activities are dependent upon specialist supplies, the organization should identify the key suppliers and single sources of supply. Strategies to manage continuity of supply may include:

— increasing the number of suppliers;

— encouraging or requiring suppliers to have business continuity;

— contractual and/or service level agreements with key suppliers; and

— the identification of alternative, capable suppliers.

Where activities are being relocated it should be verified that suppliers are able to provide their products or services effectively at the alternate location.

8.3.2.6 Information communications technology (ICT) systems

In many organizations, activities cannot be performed without ICT systems and they need to be reinstated before activities can be resumed. Where it is possible and practical, the organization may need to implement manual operations while its ICT services are being reinstated.

Technology options will depend on the nature of the technology employed and its relationship to activities, but will typically be a combination of the following:

— provision made within the organization;

— services delivered to the organization by a third party; and

— external services to which the organization subscribes.

Techniques for providing ICT systems required by prioritized activities may include:

— spreading them geographically, for example, maintaining the same technology at different locations that will not be affected by the same disruptive incident;

— holding older equipment as emergency replacement or spares; and

— contracted provision of equipment or recovery services.

Because of the complexity of the technologies that support them, ICT systems frequently need complex arrangements to ensure that they can be recovered in a timely manner. Consideration should therefore be given to:

— setting recovery time objectives (RTOs) for ICT systems that enable prioritized activities to be resumed within their RTOs;

— paying particular attention to the location of technology sites and the distance between them;

— distributing technology across a number of separate sites;

— providing adequate facilities for increased numbers of users with remote access;

— setting up un-staffed (dark) sites as well as staffed sites;

— improving telecommunications connectivity and increasing levels of redundant routing;

— providing automatic 'failover' instead of requiring manual intervention to redirect the ICT provision;

— accommodating ICT obsolescence; and

— providing additional third-party connectivity and external links.

If a technique of 'failing over' from one site to another is adopted, it may be necessary to consider the network path distance between the two sites. If there is a very long distance between the sites, this could slow down the system response and render the ICT systems ineffective.

If an organization hosts its ICT systems at more than one site, there may be an opportunity to implement a 'mutual ICT strategy' whereby each site is sized to accommodate the combined ICT capacity of more than one site.

If an organization uses very specialized or custom built technologies with long lead times it may need to consider increasing the protection of its ICT by making special previsions for replacement or restoration.

NOTE Further guidance on ICT continuity can be found in ISO/IEC 27031, ISO/IEC 27002 and ISO/IEC 20000 (both parts).

8.3.2.7 Transportation

Transportation may need to be provided after an incident for:

— staff sent home if their normal means of transport is unavailable;

— staff relocated to alternative work location; and

— resources needed at different location.

The organization should determine in advance options for providing alternative means of transport that may be required following a disruptive incident. These may include:

— identifying possible scenarios of logistic disruptions which may be caused directly by an incident and unusual situations; and

— securing alternative logistic means and routes by taking account of traffic conditions, means of transportation, and other logistics networks;

— agreements with transport providers.

8.3.2.8 Finance

The organization should determine options for ensuring that the necessary finance is available during and following a disruptive incident. This may include:

— providing funds for emergency purchases, such as, food, accommodation, facilities, consumables and transport;

— reimbursement of staff expenses;

— major expenditure on, for example, rental or purchase of buildings and equipment;

To protect against abuse or facilitate insurance claims, it may be necessary to demonstrate effective financial controls, by, for example, providing for formal recording of expenses during and following a disruptive incident.

8.3.2.9 Suppliers

If a product, service or activity has been outsourced, the responsibility and accountability for that product, service or activity remains with the organization. Consequently, an organization should ensure itself that its key suppliers have effective continuity arrangements in place. One method of doing this is to obtain evidence of the viability of key suppliers' continuity plans and their exercising and maintenance programmes. See 8.3.1.5.

8.3.3 Protection and mitigation

For identified risks requiring treatment and in line with its overall attitude to risk, the organization should consider ways of reducing the likelihood, shortening the period and limiting the impacts of disruption.

8.4 Establish and implement business continuity procedures

8.4.1 General

The organization should put in place and document procedures that provide overall control of the response to a disruptive incident and resume activities within their recovery time objectives. The business continuity procedures should establish the appropriate internal and external communications protocol and be:

a) specific – with regard to the immediate steps that should be taken during a disruption;

b) flexible – so that they may be used to respond to unanticipated threat scenarios and changing internal and external conditions;

c) focused – they should clearly relate to the impact of events that could potentially disrupt operations and be developed based on stated assumptions and an analysis of interdependencies; and

d) effective – in terms of minimizing the consequences of incidents through implementation of appropriate mitigation strategies.

8.4.2 Incident response structure

The organization should put in place procedures and a management structure that will enable it to prepare for, mitigate, and respond effectively to disruptive incidents.

The response structure should provide for:

— identifying impact thresholds that justify initiation of formal response;

— assessing the nature and extent of a disruptive incident or the potential impact;

— putting in place measures to provide for the welfare of those affected;

— initiating an appropriate response to a disruptive incident;

— having processes, and procedures for the activation, operation, coordination, and communication of the response;

— resources being available to support the processes and procedures needed to manage a disruptive incident and minimize impacts; and

— communication with interested parties, including in particular, authorities and the media.

The response structure should be simple and capable of being formed quickly. When determining the structure, consideration should be given to:

— having one or more competent personnel available to establish the ramifications of the incident and evaluate the impact or potential impact of the incident and its timescale;

— being able to mobilize teams to take control, contain the incident, and initiate the appropriate response; and

— including appropriate resources which may include staff, contractors, equipment and finance.

Larger or complex organizations may use a tiered approach to incident response and may establish different teams to focus on incident response, incident management, communications, welfare and business resumption. In smaller organizations all aspects of incident response may be handled by one team but should never be the responsibility of a single individual.

Each team should have procedures for governing its actions and include personnel with the necessary responsibility, authority and competence. Individual and team competence can be demonstrated by training and exercising.

8.4.3 Warning and communication

8.4.3.1 General

The organization should establish, implement and maintain procedures for warning and communication. These should include:

a) detecting an incident and alerting response personnel;

b) continuing monitoring of an incident;

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

d) external communications with interested parties;

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

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

g) alerting interested parties 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.

An organization may need to decide whether or not and at what point to communicate with external interested parties regarding its warning and communication procedures. Life safety should be the first consideration when making this decision. The decision and the reasons for it should be documented.

For example, an organization undertaking hazardous activities that could threaten the safety of near neighbours may need to make sure that the neighbours are notified of potential danger. This may mean that they need to understand how alarms are issued and how to respond.

The organization should have effective procedures and facilities for issuing warnings, alerts and external communication rapidly. Special arrangements may be required for interested parties with specific needs, for example, the elderly and those with disabilities. The warning and communication system should be regularly exercised. For guidance on exercising refer to 8.5.

8.4.3.2 Incident communication procedures

Procedures need to be established that, in advance of a potential incident, may enable:

— receiving, documenting and responding to any national or regional risk advisory system or equivalent; These may reflect threats that are common to the location – such as tsunami, earthquake or hurricane warnings; and

— alerting interested parties potentially impacted by an actual or impending disruptive incident – where the organization has statutory or moral responsibility for warning.

Once the incident has begun the organization should develop procedures that ensure:

— the incident is continually monitored, through local observation or remote monitoring, and any developments communicated to the appropriate responders;

— structured communication with emergency responders;

— the interoperability of multiple responding organizations and personnel where this is the responsibility of the organization;

— communication is provided between the various response teams with the organization;

— regular communication with the staff and others for whom there is a duty of care such as visitors and contractors – this may need to be at evacuation points initially then at home or alternate locations; and

— recording of vital information about the incident, actions taken and decisions made – by the individuals who made them or by an appointed log-keeper for each team.

Procedures are also required to facilitate effective two-way communication between interested parties such as customers and the media.

The organization should maintain communications with these parties until a return to normal business operations when a communication marking the end of the incident may be appropriate.

8.4.3.3 Incident communication facilities

These procedures may be facilitated by the use of a dedicated or ad hoc communications facility. This should be located sufficiently far from the affected site that its operation is not impeded by the incident and may be in the same location as other incident response facilities.

The communications equipment available should recognize that the incident may have affected the performance of normal communications so a variety of alternatives may be available such as:

— loud-hailers or public address systems;

— spare mobile phones; and

— two-way radios.

8.4.4 Business continuity plans

8.4.4.1 General

The organization should establish documented procedures that will enable the organization to respond to an incident and deal appropriately with the resumption and recovery of its activities.

These procedures should address all aspects of responding to an incident with particular regard to life safety issues and address the requirements of all those who will use them. To determine requirements, it may be beneficial to:

— involve in the development of the procedures, those who will use them;

— use feedback from exercising and lessons learned from disruptive incidents.

Timescales and performance levels should be based on the information gathered during the business impact analysis (8.2.2) and the business continuity strategy selected (8.3.1).

The following should be clearly identifiable within each plan:

— purpose and scope;

— objectives and measures of success in terms of prioritized activities;

— activation criteria and procedures;

— implementation procedures;

— roles, responsibilities, and authorities;

— communication requirements and procedures;

— internal and external interdependencies and interactions;

— resource requirements; and

— information flow and documentation processes.

When dealing with a disruptive incident, there are number of actions that may need to be considered. These should be included in documented procedures (8.4.4.2 and 8.4.4.3) and include:

a) responding to and assessing the incident:

   1) What happened and how did it occur?

   2) Which parts of the organization and which interested parties have been or could have been affected?

   3) What is the anticipated duration of the incident and its impacts? and

   4) May the incident be managed by routine management arrangements?

b) evaluating the incident assessment against activation criteria for each of the procedures;

c) declaring an incident and activating the procedures when activation criteria have been met;

d) stabilization, continuity, resumption and recovery activities;

e) establishing and running the incident management location;

f) prioritizing issues and activities to be undertaken in managing the incident and its impacts;

g) controlling and coordinating all activated procedures;

h) activating or establishing alternate sites for the restoration of IT or other infrastructure capability and for the temporary operation of the organization's activities;

i) monitoring the incident as it progresses;

j) reviewing and adapting plans in response to changing circumstances;

k) standing down of plans and return to routine management as sustainable capability is re-established;

l) conducting a debrief and identifying learning opportunities; and

m) ensuring good governance and collation and security of documentation generated during the management and recovery from the incident.

To achieve the timely resumption of the organization's delivery of products and services, the documented procedures for resuming each activity should:

— meet the recovery time objective of the activity which supports that product or service; and

— be sufficiently reliable.

This may be achieved by:

— ownership or control of the means and resource to enact the procedure; and

— contracts, agreements or service levels with third parties.

To ensure that the operation of the procedures is not affected by the same disruption, the organization may take precautions, for example, separating personnel and ICT across multiple locations. However, total separation for all scales and types of incident is not possible and this limitation should be identified and agreed with top management. This limitation could be expressed in terms of distance, minimum personnel or severity and may be determined by the response of civil authorities to a severe and/or widespread incident.

8.4.4.2 Content of business continuity plans

A business continuity plan may be a single documented procedure or multiple procedures encompassing all requirements and covering the scope of the BCMS.

The purpose, scope and objectives of each documented procedure should be defined and be understandable to those who will put it into effect. Any relationship to other required and relevant documented procedures or documents should be clearly referenced and the method of obtaining and accessing them described.

Within the business continuity plans the following should be clearly identifiable (see also 8.4.4.3):

a) roles and responsibilities:

   1) defined roles, responsibilities and authorities for people and teams who will use the business continuity plan. If the business continuity plan comprises more than one documented procedure, the roles, responsibilities and authorities for each procedure should be defined; and

   2) guidelines and criteria regarding who has the authority to invoke the procedures and under what circumstances – this may follow defined escalation stages.

b) invocation and standing down:

   1) a process for activating the organization's response to a disruptive incident and within each documented procedure, its activation criteria and procedures. It may be relevant to consider whether this is within or outside normal working hours;

   2) a process for standing teams down once the incident has passed; and

3) rendezvous and places to meet with suitable alternatives.

c) incident management:

1) management of the immediate consequences of a disruptive incident giving due regard to welfare issues of affected persons (including team members), options for responding to the disruption (these may be described as strategic, tactical and operational) and prevention or further loss or unavailability of prioritized activities;

2) within each documented procedure there should be:

i) implementation procedures that identify actions and tasks that need to be performed, particularly in relation to how the organization will continue or recover its prioritized activities within predetermined timeframes;

ii) resource requirements (8.3.2) relevant to the documented procedure; and

iii) the means for recording key information about the incident, actions taken and decisions made.

d) contact information within each documented procedure:

1) contact details for team members and others with roles and responsibilities – where local data protection legislation applies, contact details should be held in accordance with it; and

2) contact and mobilization details for any relevant agencies, organizations and resources that might be needed.

e) communication (8.4.3):

1) details addressing how and under what circumstances the organization will communicate with employees and their relatives, key interested parties and emergency contacts; and

2) details of the organization's media response following an incident, including its communication strategy, preferred interface with the media, guidelines or templates for drafting media statements and identification of appropriate spokespeople.

8.4.4.3 Specific types of procedures

8.4.4.3.1 Incident management / strategic management procedures

The aim of incident management is to ensure that the organization's response to a disruptive incident is effective at a strategic level.

The procedures should include the basis for managing all possible issues facing the organization during an incident, including those related to interested parties.

The organization should identify a location, room or space from which an incident will be managed. Once established, this location should be the focal point for the organization's response. An alternative meeting point at a different location should also be nominated in case access to the primary location is denied. Each location should have access to appropriate resources by which the incident management team may initiate effective incident management activities without delay.

The location may be as simple as a hotel room or a staff member's house. It may be as complex as a dedicated 'command centre' with PCs, video-conferencing and multiple telephones. Initially, it might be necessary to hold a virtual or off-site meeting, e.g. via telephone, teleconference or videoconference, so that key decisions may be made promptly.

The chosen location should be fit-for-purpose and may include:

— space for the required number of people;

— effective primary and secondary means of communication; and

— facilities for accessing and sharing information, including the monitoring of the news media.

Other response teams may require similar facilities.

8.4.4.3.2 Communications procedures

Communications procedures may be included in incident management response procedures or may be separated for use by a separate team as appropriate.

There is a need to manage and coordinate actively the many communications that will be delivered and received during the incident. This procedure should contain:

a) details on how and under what circumstances the organization will communicate with employees and their relatives, emergency contacts and other interested parties';

b) details on the organization's media response following an incident, including:

   1) the incident communications strategy;

   2) preferred interface with the media;

   3) guideline or template for drafting a statement for the media; and

   4) appropriate numbers of trained, competent spokespeople authorized to release information to the media.

Prepared information may be especially useful in the early stages of an incident. It enables an organization to provide details about the organization and its business while details of the incident are still being established.

It may be appropriate to:

— establish a suitable venue to support liaison with the media, or other groups of interested parties;

— establish an appropriate number of competent, trained people to answer telephone enquiries from the press;

— use all communication channels open to the organization including social media; and

— prepare background material about the organization and its operations (this information should be pre-agreed for release).

Pressure or community action groups who collectively have power or influence over the organization may also need to be considered.

A process for identifying and prioritizing communications with other key interested parties should be included. It may be necessary to develop a separate procedure for managing interested parties, provide criteria for setting priorities and make provisions for allocating persons to each stakeholder or group of stakeholders.

8.4.4.3.3 Safety and welfare procedures

Organizations have a direct responsibility to safeguard the welfare of employees, contractors, visitors and customers where an incident poses a direct risk to life, livelihood and welfare. Special attention will need to be paid to any groups with disabilities or other specific needs (e.g. pregnancy, temporary disability due to injury). Planning in advance to meet these requirements may reduce risk and reassure those affected. The long-term impacts of incidents cannot be underestimated. Developing appropriate strategies in support of human welfare may directly promote physical and emotional recovery within the organization and these should take into account relevant social and cultural considerations.

Elements of welfare response that should be included:

— site evacuation (inclusive of internal 'shelter-at-site' activities) and assembly points;

— the mobilization of safety, first aid or evacuation-assistance teams; and

— locating and accounting for those who were on site or in the immediate vicinity.

The following may also be included:

— translation services;

— transport assistance including directions as required;

— designated liaisons and contact information for emergency services, appropriate agencies, and first responders;

— locating displaced workforce or contractors;

— managing telephone help lines; and

— rehabilitation and counselling services (physical and emotional).

The organization may retain a means to provide services to debrief and counsel affected staff after an incident and to provide long-term support. Services may be sourced externally or may be provided as an extension to existing occupational health and employee assistance programmes.

The organization should deploy staff with appropriate levels of authority to liaise where appropriate with the emergency services. Emergency services play the primary role in protecting life and relieving suffering during emergencies. Therefore, early liaison, pre-planning and real-time incident coordination between the organization and its first responders and the emergency services may improve the efficiency of an incident response.

Any required resources should be specifically identified. A resource should be available in a timely manner and should have the capability to do its intended function. Restriction on the use of the resource should be taken into account, and application of the resource should not incur more liability than would failure to use the resource. The cost of the resource should not outweigh the benefit.

The resources that may be required for welfare response include, but are not limited to, the following:

— the locations, quantities, accessibility, operability, and maintenance of equipment (e.g. heavy duty, protective, transportation, monitoring, decontamination, response, personal protective equipment);

— supplies (e.g. medical, personal hygiene, consumable, administrative, ice);

— sources of energy (e.g. electrical, fuel);

— emergency power production (generators);

— communications systems;

— food and water;

— technical information;

— clothing and shelter;

— specialized personnel (e.g. medical, religious, volunteer organizations, disaster/emergency management staff, utility workers, morticians, and private contractors);

— specialized volunteer groups (e.g. amateur radio, religious relief organizations, charitable agencies);

— volunteer, community, and emergency response support; and

— external international, national, provincial, tribal, territorial, and local agencies.

8.4.4.3.4 Salvage and security procedures

The organization may prepare documented procedures that address salvage and security. This may include guidance on:

— salvage priorities for facilities, equipment and documented information; and

— security of the premises once handed over by the emergency services.

— the organization may appoint specialist salvage contractors in advance of the incident. Effective salvage of facilities, equipment and documented information may limit impacts and enable a more rapid return to normal working.

8.4.4.3.5 Procedures for resuming activities

Each procedure should specify the:

— prioritized activities to be resumed;

— timescales within which they are to be resumed;

— recovery levels needed for each prioritized activity; and

— situations in which the procedure may be utilized.

Each should detail where appropriate, the resources required at different points in time to achieve the objectives. This may include:

— resource numbers;

— skills and qualifications;

— technical equipment;

— telecommunications facilities; and

— availability of resources contracted, agreed through mutual aid or likely to be available.

In the event that lack of a service or resource threatens the resumption of activities, escalation actions should be defined. These actions may include:

— mobilization of external and third-party resources;

— communication of recovery actions; and

— procedures for implementing manual workarounds, system recovery, alternative processes etc.

Resource requirements should be documented and may include:

— vital records (hardcopy and electronic);

— operating and procedure manuals;

— IT technical recovery plans and procedures;

— location of offsite storage facilities being used by the organization;

— alternative locations;

— authorities/delegations for the payment of emergency expenses;

— a list of staff with expertise required by the operational units;

— IT infrastructure and applications documentation;

— telecommunications support source;

— office and specialist equipment sources; and

— utilities (water, power etc.) contacts.

8.4.4.3.6 Recovery of information communications technology (ICT) systems

The procedures for resuming activities should identify the ICT systems on which their resumption relies and reference any ICT continuity procedures that exist.

ICT continuity procedures, if any, should at minimum address:

— invocation of the required ICT response and recovery and deployment of ICT personnel;

— accessing back-up data and acquiring alternative service provision; and

— restoration of data, information services and communications and support;

— the timetable of availability and capacity requirements set out in the business continuity procedures allowing activities to meet their recovery time objectives.

NOTE Further guidance can be found in ISO 27031.

8.4.5 Recovery

The organization should have documented procedures to restore and return business operations from the temporary measures adopted to support normal business requirements after an incident. These should address relevant audit and corporate governance requirements.

The purpose of recovery is to re-establish business activities to support normal business requirements following a disruptive incident. Returning to normal may be achieved by:

— repairing the damage resulting from the incident;

— migrating operations from temporary premises back to the restored primary business location; or

— moving to a new location.

A decision on how best to 'return to normal' will need to be taken based on the severity of the damage caused by the incident and estimates of how long it might take to establish the necessary facilities.

The documented procedures should provide for a detailed assessment of the situation and its impact and the determination of tasks and steps needed for recovery. During recovery, the organization may need to:

a) establish recovery resources and infrastructure;

b) operate at recovery facilities;

c) restore damaged facilities;

d) secure emergency procurement and funding;

e) salvage equipment in damaged facilities;

f) make claims against existing insurance policies;

g) obtain additional manpower to support the recovery effort;

h) select options for restoring and returning to normal;

i) migrate operations to recovery facilities;

j) recover lost documented information;

k) communicate with relevant interested parties at appropriate frequencies;

l) normalize operations at the restored facilities;

m) conduct a post recovery review; and

n) conduct due diligence on audit and corporate governance requirements.

The documented procedures for recovery should include provision for the resumption of all activities and not just those identified as prioritized activities. This recognizes that activities with a lower priority need to be resumed at some point in time and have resource requirements (8.3.2).

8.5 Exercising and testing

8.5.1 General

An organization's business continuity procedures and arrangements cannot be considered reliable until exercised and unless their currency is maintained. Exercising is essential to ensure that the strategies, policies, plans and procedures that have been put in place are adequate and meet the business continuity objectives. Exercising develops teamwork, competency, confidence and knowledge and should include those who may be required to use the procedures.

8.5.2 Exercise programme

No matter how well designed and thought-out a procedure appears to be, a series of robust and realistic exercises will identify areas for improvement.

An exercise programme should be consistent with the scope of the business continuity procedures, giving due regard to any relevant legislation and regulation.

An exercise programme should be devised that will demonstrate, over a period of time, objective assurance that the business continuity procedures and arrangements will work as anticipated when required. The programme should:

a) exercise the technical, logistical, administrative, procedural and other operational systems of the procedures;

b) exercise all persons with responsibilities within those procedures;

c) exercise the business continuity arrangements and infrastructure (including, for example, incident management locations and work areas); and

d) validate the technology and telecommunications recovery, including the availability and relocation of staff.

The scale and complexity of exercises should be appropriate to the organization's business continuity objectives.

There should be a planned schedule of exercises, the frequency of which should depend on the organization's needs, the environment in which it operates and the requirements of interested parties. However, the exercising programme should be flexible, taking into account changes within the organization and the outcome of previous exercises. A significant change in the organization may trigger the scheduling of an exercise to examine the revised arrangements.

The exercise programme should consider the roles of all parties, including key third party providers, suppliers and others who would be expected to participate in recovery activities. An organization may include such parties in its exercises and may participate in exercises that they organize.

The scope and detail of the exercises should mature through the programme based on the organization's experience, resources, and capabilities. At early stages of maturity, exercising and testing may be limited

to the use of checklists, drills and awareness exercises. As the programme matures, it may extend to include table top exercises and full-scale live simulations.

8.5.3 Exercising business continuity plans

Exercises are activities designed to examine the organization's ability to respond, recover and continue to perform assigned business functions effectively when faced with specific disruptive scenarios. The organization should use exercises and the documented results of exercises to ensure the effectiveness and readiness of its business continuity plans.

Every exercise and test should have clearly defined aims and objectives and be based on a scenario that is appropriate to meeting them.

Exercises may:

— anticipate a predetermined outcome, e.g. are planned and scoped in advance; and

— allow the organization to develop innovative solutions.

Exercises should be realistic, carefully planned and agreed with relevant parties, so that there is minimum risk of disruption to business processes and of an incident occurring as a direct result of the exercise. This may be achieved by undertaking the exercise within a controlled and isolated environment provided this does not jeopardize the integrity of the objectives being tested.

The organization should design exercise scenarios that satisfy the objectives of the exercise and may use threats identified in the risk assessment or other appropriate events.

The effectiveness of some aspects of business continuity will require that particular individuals or those occupying specific positions have particular knowledge, skills and understandings. These should be in place before the exercise allowing the participants to apply them to relevant scenarios and simulations.

Exercises should be designed and conducted so that they provide one or more of the following:

a) verification that recovery time objectives are achievable (8.3.1);

b) confidence that information required by activities is appropriately current (8.3.2.3);

c) improved understanding of dependencies on the business continuity of suppliers, and other interested parties;

d) improved awareness of the organizational context and priorities;

e) improved understanding of the content and use of business continuity procedures;

f) improved confidence in responding to incidents;

g) an opportunity to improve capabilities;

h) an assessment of the utility and applicability of business continuity strategies;

i) an evaluation of the adequacy of developed capabilities and resource allocations;

j) an identification of previously undocumented requirements and practices employed in managing an incident or disruption;

k) an opportunity to identify any other inadequacies in the written business continuity procedures and their implementation;

l) assurance that business continuity procedures are capable of being implemented when required;

m) improved confidence of interested parties regarding the organization's preparedness; and

n) a means of fulfilling regulatory, contractual or organizational governance requirements.

Exercises may be in a variety of different formats. The decision as to the suitability of the type of exercise will depend upon the context for BCM, the objectives for the exercise, budget and participant availability and the tolerance of the organization to operational disruption caused by holding the exercise.

The principal types of exercise are described in ISO 22398 (Societal security – Guidelines for exercises and testing).

As part of the exercise, a review should be scheduled with all participants to discuss issues and lessons learned. This information should be documented and updates made to the procedures as required.

The organization should undertake a post-exercise debriefing and analysis that considers the achievement of the aims and objectives of the exercise. A post-exercise report should be produced that contains recommendations and a timetable for their implementation.

Lessons from exercises and actual incidents experienced should be re-examined during future exercises. Exercises that show serious deficiencies or inaccuracies in the procedures should be rerun after corrective actions have been completed.

Benefits of exercising and testing include:

— validation of planning scope, assumptions and strategies;

— assurance of the correct functioning of technical facilities and resources;

— assurance of the capacity of the alternate facilities;

— increased efficiency and reductions in the time needed to complete processes (e.g. using repeated drills to shorten response times);

— interested parties' improved awareness; and

— development of participants' competency and awareness.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.1.1 General

The procedures for the performance and the effectiveness of the BCMS should include setting of performance metrics; assessment of the protection of prioritized activities; confirmation of compliance with requirements; examination of historical evidence; and use of documented information to facilitate subsequent corrective actions. Procedures should also reference business continuity policy and objectives.

The procedures for monitoring performance should include the following:

a) setting of performance metrics including qualitative and quantitative measurements that are appropriate to the needs of the organization;

b) monitoring the extent to which the organization's business continuity policy and objectives are met;

c) identifying when the monitoring and measuring should take place;

d) assessing the performance of the processes, procedures and functions that protect prioritized activities;

e) proactive measures of performance that monitor compliance of the BCMS with applicable legislation, statutory and regulatory requirements;

f) reactive measures of performance to monitor failures, incidents, non-conformances (including near misses and false alarms) and other historical evidence of deficient BCMS performance; and

g) recording data and results of monitoring and measurement sufficient to facilitate subsequent corrective action analysis.

The procedures should provide for systematic measurement, monitoring and evaluation of the organization's business continuity on a regular basis. A set of performance indicators should be developed to measure both the management system and its outcomes. Measurements may be either quantitative or qualitative. Performance indicators may be management, operational, or economic indicators. Indicators should provide useful information to identify both successes and areas requiring correction or improvement.

The BCMS should provide data from monitoring and measurement to identify patterns and obtain information regarding its performance. This data should be used to ensure that the organization's policy and objectives are achieved as well as identifying corrective actions and areas for improvement.

The organization should be able to demonstrate that it has identified, evaluated and complied with the legal requirements and any other requirements to which it has subscribed.

Records of all periodic evaluations and their results should be maintained.

The organization should analyse, and at planned intervals, evaluate the outcomes from the monitoring and measurement.

9.1.2 Evaluation of business continuity procedures

The organization should conduct evaluations of its business continuity procedures in order to ensure their continuing suitability, adequacy and effectiveness.

The evaluations should address the possible need for changes to policy, objectives, strategies, and other elements of the BCMS in the light of such things as exercise results, post-incident reviews, changing circumstances and the commitment to continual improvement.

Evaluations may take the form of internal or external audits, or self-assessments. The frequency and timing of reviews may be influenced by laws and regulations, depending on the size, nature and legal status of the organization. They might also be influenced by the requirements of interested parties.

An evaluation of the organization's business continuity procedures should verify that:

a) all key products and services and their supporting activities and resources have been identified and included in the organization's business continuity strategy;

b) the organization's business continuity policy, strategies, framework and business continuity procedures accurately reflect its priorities and requirements (the organization's objectives);

c) the competence of persons and the organization's business continuity are effective and fit-for-purpose and will permit management, command, control and coordination of the organization's response to a disruptive incident;

d) the organization's business continuity solutions are effective, up-to-date and fit-for-purpose, and appropriate to the level of risk faced by the organization;

e) the organization's business continuity maintenance and exercising programmes have been effectively implemented;

f) business continuity strategies and procedures incorporate improvements identified during incidents and exercises and in the maintenance programme;

g) the organization has an on-going programme for business continuity training and awareness;

h) business continuity procedures have been effectively communicated to relevant staff, and that those staff understand their roles and responsibilities; and

i) change control processes are in place and operate effectively.

A clearly defined and documented maintenance programme should be established. This programme should:

— ensure that any changes (internal or external) that impact the organization are reviewed in relation to BCM;

— identify any new products and services and their dependent activities that need to be included in the BCMS;

— ensure that the organization's business continuity remains effective, fit-for purpose and up-to-date; and

— enable existing exercise schedules to be modified when there has been a significant change in any of the business continuity strategies or associated business processes.

NOTE An effective way of assessing the impact of major business changes, is for the organization to review the business impact analysis (8.2.2) at the earliest opportunity and based on the outcome make changes to other elements of BCM

The outcomes from the maintenance process should include:

— documented evidence of the proactive management and governance of the organization's BCM;

— verification that key people who are to implement the business continuity strategy and procedures are trained and competent;

— verification of the operational planning and control of BCM;

— evidence that the organization has evaluated compliance of its business continuity procedures; and

— evidence that significant changes to the organization's structure, products and services and activities have been reflected in the organization's business continuity procedures in a timely manner.

In the event of an incident that disrupts the organization's prioritized activities or requires an incident response, a post-incident review should be undertaken. This may include:

— identifying the nature and cause of the incident;

— assessing the adequacy of management's response;

— assessing the organization's effectiveness in meeting its recovery time objectives;

— assessing the adequacy of the business continuity arrangements in preparing employees for the incident;

— identifying improvements to be made to the business continuity arrangements;

— comparing actual impacts with those considered during the business impact analysis (8.2.2); and

— obtaining feedback from interested parties and those who have participated in the response.

In the context of continual improvement, the organization may acquire knowledge on new BCM technology and practices, including new tools and techniques. These should be evaluated to establish their potential benefit to the organization.

Documented information relating to all periodic evaluations and their results should be maintained as evidence of the evaluations.

9.2 Internal audit

The organization should conduct internal audits at planned intervals so that it may make sure the BCMS conforms to its own requirements and the requirements of this International Standard.

It is essential to conduct internal audits of the BCMS to ensure that the BCMS is achieving its objectives, conforms to its planned arrangements and has been properly implemented and maintained, and to identify opportunities for improvement. Internal audits of the BCMS should be conducted at planned intervals

to determine and provide information to top management on appropriateness and effectiveness of the BCMS as well as to provide a basis for setting objectives for continual improvement of BCMS performance.

The organization should establish an audit programme (see ISO 19011) to direct the planning and conduct of audits, and identify the audits needed to meet the programme objectives. The programme should be based on the nature of the organization's activities, in terms of its risk assessment and impact analysis, the results of past audits, and other relevant factors.

An internal audit programmes should be based on the full scope of the BCMS, however, each audit need not cover the entire system at once. Audits may be divided into smaller parts, so long as the audit programme ensures that all organizational units, functions, activities and system elements and the full scope of the BCMS are audited in the audit programme within the auditing period designated by the organization.

The results of an internal BCMS audit may be provided in the form of a report and used to correct or prevent specific nonconformities and provide input to the conduct of the management review.

Internal audits of the BCMS may be performed by personnel from within the organization or by external persons selected by the organization, working on its behalf. In either case, the persons conducting the audit should be competent and in a position to do so impartially and objectively. In smaller organizations, auditor independence may be demonstrated by an auditor being free from responsibility for the activity being audited.

9.3 Management review

Top management should review the organization's BCMS, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness including the effective operation of its continuity procedures and capabilities.

Management review should include appraisal of:

— the status of actions from previous reviews;

— the performance of the management system including trends apparent from nonconformities and corrective actions, the results of monitoring and measurement, and audit findings;

— changes to the organization and its context (4.1) that might impact the management system; and

— opportunities for continual improvement.

Management review provides top management with the opportunity to evaluate the continuing suitability, adequacy and effectiveness of the management system. The management review should cover the scope of the BCMS, although it is not necessary to review all elements at once and the review process may take place over a period of time.

Review of the implementation and outcomes of the BCMS by top management should be regularly scheduled and evaluated. While on-going system review is advisable, formal review should be structured and appropriately documented and scheduled on a suitable basis. Persons who are involved in implementing the BCMS and allocating its resources should be involved in the management review.

In addition to the regularly scheduled management system reviews, the following factors may trigger a review and should otherwise be examined once a review is scheduled:

a) **Sector/industry trends**: Major sector/industry initiatives should initiate a BCMS review. General trends and best practices in the sector/industry and in business/operational continuity planning techniques may be used for benchmarking purposes;

b) **Regulatory requirements**: New regulatory requirements may require a review of the BCMS; and

c) **Incident experience**: A review should be performed following a response to a disruptive incident, whether or not the response procedure was activated. If activated, the review should take into

account the history of the response procedure, how it worked, why it was activated, etc. If the response procedure was not activated, the review should examine why this was and whether or not it was an appropriate decision;

A management review should result in improvements to the efficiency and performance of the BCMS and may result in the following changes:

— variations to the scope;

— improvements in its effectiveness;

— updates to business continuity procedures; and

— changes to controls and how their effectiveness is measured.

The organization should retain documented information as evidence of the results of management reviews and should:

— communicate the results of management review to relevant interested parties; and

— take appropriate action relating to those results.

10 Improvement

10.1 Nonconformity and corrective action

The organization should identify nonconformities, take action to control, contain and correct them, deal with their consequences and evaluate the need for action to eliminate their causes.

The organization should establish effective procedures to ensure that non-fulfilment of a requirement, planning approach and weaknesses associated with the BCMS are identified and communicated in a timely manner to prevent further occurrence of the situation, as well as identify and address root causes. The procedures should enable on-going detection, analysis and elimination of actual and potential causes of non-conformities.

Non-conformances should be identified and dealt with in a timely manner as should the corrective actions that address them. The corrective action may originate from a well-defined nonconformity statement that clearly states the problem and is understood.

When any nonconformity is identified, an investigation into its root cause should be conducted and a corrective action plan developed for immediately addressing the problem. The action plan should be designed to mitigate any consequences and identify changes to be made to correct the situation, restore normal operations and eliminate the cause(s) in order to prevent the problem from recurring. The nature and timing of actions should be appropriate to the scale and nature of the nonconformity and its potential consequences.

A potential problem may be identified but no actual nonconformity exists. Potential problems may be extrapolated from corrective actions for actual nonconformities, identified during the internal BCMS audit process or analysis of industry trends and events. Identification of potential nonconformities may also be made part of routine responsibilities of persons aware of the importance of noting and communicating potential or actual problems.

Establishing procedures for addressing actual and potential nonconformities and for taking corrective actions on an on-going basis helps to ensure reliability and effectiveness of the BCMS. The procedures should define responsibilities, authority and steps to be taken in planning and carrying out corrective action. Top management should ensure that corrective actions are implemented and that there is systematic follow-up to evaluate their effectiveness.

10.2 Continual improvement

The organization should continually improve the effectiveness of the BCMS.

Continual improvement operates at all levels within the PDCA cycle and should be driven by the business continuity policy and objectives, audit results, analysis of monitored events, corrective actions and management review.

Changes arising from corrective actions should be reflected in BCMS documentation.

Continual improvement requires a process that properly identifies problems and non-conformances and then fixes them. This process should address the nature of the problem and the environment within which the problem exists and include changing the environment to ensure that the problem doesn't recur. Each step should build and improve on the previous step so that improvement covers more aspects than just the original identified problem and has a wider, more telling effect on the organization.

The implementation of corrective actions should be validated as effective. Each action should have an estimated date of completion. After that date, the organization should ensure that the prescribed action was accomplished and effective. If the review reveals the action did not succeed as planned, a new date for action should be set.

The continual improvement process should follow the same basic process as used for corrective actions and include the following:

— identify what to address and the present condition (non-conformance);

— identify the present process and controls (root cause); and

— determine what changes to implement (corrective action).

Corrective actions address deficiencies in the BCMS and ensure that it functions as intended, while continual improvement takes the BCMS to a higher level of efficiency and effectiveness.

Bibliography

[1] ISO 19011:2011, *Guidelines for auditing management systems*

[2] ISO 20000 (all parts), *Information technology — Service management*

[3] ISO 22398[1)], *Societal security — Guidelines for exercises*

[4] ISO/PAS 22399:2007, *Societal security — Guideline for incident preparedness and operational continuity management*

[5] ISO 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

[6] ISO 27031:2011, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[7] ISO 31000:2009, *Risk management — Principles and guidelines*

[8] BSI 25999-1:2006, *Business continuity management — Code of practice*

[9] BSI 25999-2:2007, *Business continuity management — Specification*

[10] HB 221:2004, *Business continuity management*, Standards Australia/Standards New Zealand, ISBN 0-7337-6250-6

[11] SI 24001:2007, *Security and continuity management systems — Requirements and guidance for use*, Standards Institution of Israel

[12] NFPA. 1600:2007, *Standard on disaster/emergency management and business continuity programs,* National Fire Protection Association (USA)

[13] *Business Continuity Plan Drafting Guideline*. Ministry of Economy, Trade and Industry, Japan, 2005

[14] *Business Continuity Guideline*, Central Disaster Management Council, Cabinet Office, Government of Japan, 2005

[15] ANSI/ASIS SPC.1:2009, *Organizational Resilience: Security, Preparedness, and Continuity Managements Systems – Requirements with Guidance for Use*

[16] ANSI/ASIS/BSI BCM.01:2010, *Business Continuity Management Systems: Requirements with Guidance for Use*

[17] SS 540: 2008, *Singapore Standard for Business Continuity Management*

1) To be published.

ICS 03.100.01

Price based on 46 pages