ICS 03.100.01 SLOVENSKÁ TECHNICKÁ NORMA Jún 2020

STN	**Ochrana spoločnosti Systémy manažérstva plynulosti podnikania Usmernenie (ISO 22313: 2020)**	**STN EN ISO 22313 83 0003**

Security and resilience - Business continuity management systems - Guidance on the use of ISO 22301 (ISO 22313:2020)

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 05/20

Obsahuje: EN ISO 22313:2020, ISO 22313:2020

Oznámením tejto normy sa ruší
STN EN ISO 22313 (83 0003) z apríla 2015

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 22313

February 2020

ICS 03.100.01; 03.100.70

Supersedes EN ISO 22313:2014

English Version

Security and resilience - Business continuity management systems - Guidance on the use of ISO 22301 (ISO 22313:2020)

Sécurité et résilience - Systèmes de management de la continuité d'activité - Lignes directrices sur l'utilisation de l'ISO 22301 (ISO 22313:2020)

Sicherheit und Resilienz - Business Continuity Management Systems - Anleitung zur Verwendung von ISO 22301 (ISO 22313:2020)

This European Standard was approved by CEN on 18 February 2020.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. EN ISO 22313:2020 E

EN ISO 22313:2020 (E)

Contents

Page

European foreword

This document (EN ISO 22313:2020) has been prepared by Technical Committee ISO/TC 292 "Security and resilience" in collaboration with Technical Committee CEN/TC 391 “Societal and Citizen Security” the secretariat of which is held by AFNOR.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by August 2020, and conflicting national standards shall be withdrawn at the latest by August 2020.

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

This document supersedes EN ISO 22313:2014.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 22313:2020 has been approved by CEN as EN ISO 22313:2020 without any modification.

INTERNATIONAL STANDARD

ISO 22313

Second edition
2020-02

Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301

Sécurité et résilience — Systèmes de management de la continuité d'activité — Lignes directrices sur l'utilisation de l'ISO 22301

Reference number
ISO 22313:2020(E)

ISO 22313:2020(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

This second edition cancels and replaces the first edition (ISO 22313:2012), which has been technically revised. The main changes compared with the previous edition are as follows:

— structural and content alterations have been made to align this document with the latest edition of ISO 22301;

— additional guidance has been added to explain key concepts and terms;

— content has been removed from 8.4 that will be included in ISO/TS 22332 (under development).

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

0.1 General

This document provides guidance, where appropriate, on the requirements specified in ISO 22301. It is not the intention of this document to provide general guidance on all aspects of business continuity.

This document includes the same clause headings as ISO 22301 but does not restate the requirements and related terms and definitions.

The intention of the guidance is to explain and clarify the meaning and purpose of the requirements of ISO 22301 and assist in the resolution of any issues of interpretation. Other International Standards and Technical Specifications that provide additional guidance, and to which reference is made in this document, are ISO/TS 22317, ISO/TS 22318, ISO 22322, ISO/TS 22330, ISO/TS 22331 and ISO 22398. The scope of these documents can extend beyond the requirements of ISO 22301. Organizations should therefore always refer to ISO 22301 to verify the requirements to be met.

To provide further clarification and explanation of key points, this document includes several figures. The figures are for illustrative purposes only and the related text in the body of this document takes precedence.

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

— establishing business continuity policy and objectives that align with the organization's objectives;

— operating and maintaining processes, capabilities and response structures for ensuring the organization will survive disruptions;

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

— continual improvement based on qualitative and quantitative measurement.

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

a) a policy;

b) competent people with defined responsibilities;

c) management processes relating to:

   1) policy;

   2) planning;

   3) implementation and operation;

   4) performance assessment;

   5) management review;

   6) continual improvement;

d) documented information supporting operational control and enabling performance evaluation.

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.

0.2 Benefits of a business continuity management system

A BCMS increases the organization's level of preparedness to continue to operate during disruptions. It also results in improved understanding of the organization's internal and external relationships, better communication with interested parties and the creation of a continual improvement environment. There are potentially many additional benefits to implementing a BCMS in accordance with the recommendations contained in this document and in accordance with the requirements of ISO 22301.

— Following the recommendations in Clause 4 ("context of the organization") involves the organization:
  — reviewing its strategic objectives to ensure that the BCMS supports them;
  — reconsidering the needs, expectations and requirements of interested parties;
  — being aware of applicable legal, regulatory and other obligations.
— Clause 5 ("leadership") involves the organization:
  — reconsidering management roles and responsibilities;
  — promoting a culture of continual improvement;
  — allocating responsibility for performance monitoring and reporting.
— Clause 6 ("planning") involves the organization:
  — re-examining its risks and opportunities and identifying actions to address and take advantage of them;
  — establishing effective change management.
— Clause 7 ("support") involves the organization:
  — establishing effective management of its BCMS resources, including competence management;
  — improving employee awareness of matters that are important to management;
  — having effective mechanisms for internal and external communications;
  — managing its documentation effectively.
— Clause 8 ("operation") results in the organization considering:
  — the unintended consequences of change;
  — business continuity priorities and requirements;
  — dependencies;
  — vulnerabilities from an impact perspective;
  — risks of disruption and identifying how best to address them;
  — alternative solutions for running the business with limited resources;
  — effective structures and procedures for dealing with disruptions;
  — responsibilities to the community and other interested parties.
— Clause 9 ("performance evaluation") involves the organization:
  — having effective mechanisms for monitoring, measuring and evaluating performance;

— involving management in monitoring the performance and contributing to the effectiveness of the BCMS.

— Clause 10 ("improvement") involves the organization:

— having procedures for monitoring performance and improving effectiveness;

— benefitting from continual improvement of its management systems.

As a result, implementation of the BCMS can:

a) protect life, assets and the environment;

b) protect and enhance the organization's reputation and credibility;

c) contribute to the organization's competitive advantage by enabling it to operate during disruptions;

d) reduce costs arising from disruptions and improving the organization's capability to remain effective during them;

e) contribute to the organization's overall organizational resilience;

f) assist in making interested parties more confident in the organization's success;

g) reduce the organization's legal and financial exposure;

h) demonstrate the organization's ability to manage risk and address operational vulnerabilities.

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

This document 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. An explanation of the PDCA cycle is given in Table 1.

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

Table 1 — Explanation of PDCA cycle

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 policy and objectives, 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.

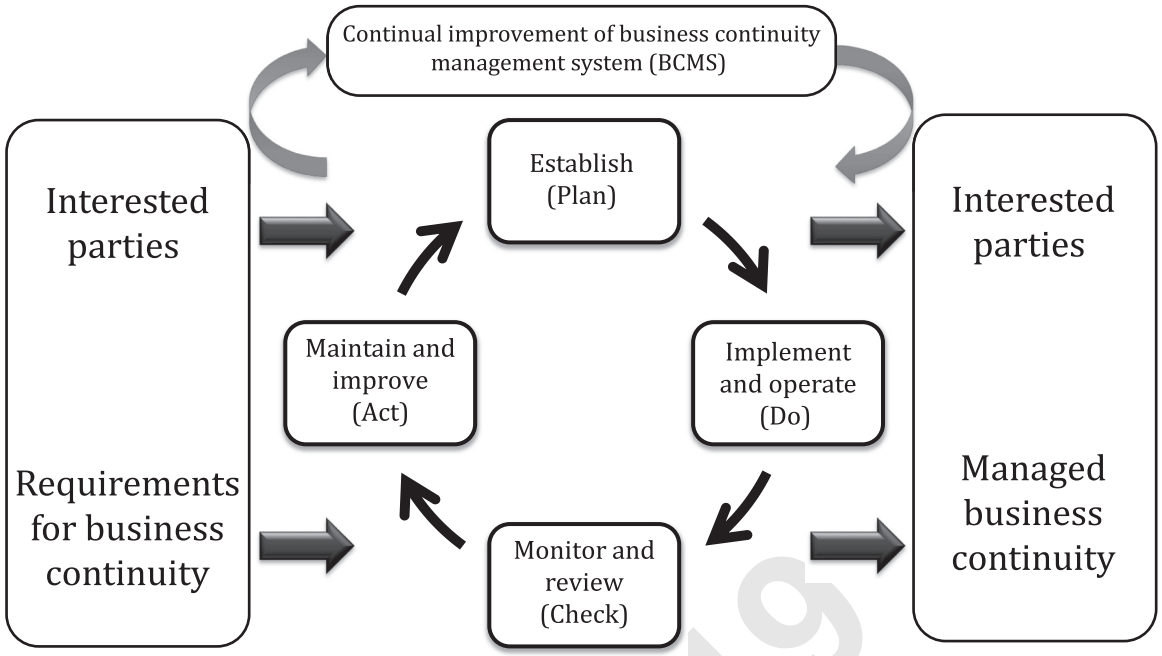

Figure 1 — PDCA cycle applied to BCMS processes

0.4 Components of PDCA in this document

Table 2 shows the direct relationship between the content of Figure 1 and the clauses of this document.

Table 2 — Relationship between the PDCA cycle and Clauses 4 to 10

PDCA component	Clause addressing PDCA component
Plan (Establish)	Clause 4 ("context of the organization") sets out what the organization should 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 role of management in terms of demonstrating commitment, defining policy and establishing roles, responsibilities and authorities.
	Clause 6 ("planning") describes the actions for establishing strategic objectives and guiding principles for the implementation of the BCMS.
	Clause 7 ("support") identifies the BCMS elements that should be in place, namely: resources, competence, awareness, communication and documented information.
Do (Implement and operate)	Clause 8 ("operation") identifies the processes for establishing and maintaining business continuity.
Check (Monitor and review)	Clause 9 ("performance evaluation") provides the basis for improving the BCMS through measurement and evaluating its performance.
Act (Maintain and improve)	Clause 10 ("improvement") covers the corrective action for addressing nonconformity identified through performance evaluation.

0.5 Contents of this document

It is not the intent of this document 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, particularly customers and employees. 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 document is not intended to be used to assess an organization's ability to meet its own business continuity needs, or any customer, legal or regulatory needs. Organizations wishing to do so can use the requirements in ISO 22301.

Clauses 1 to 3 in this document set out the scope, normative references and terms and definitions that apply to the use of this document. Clauses 4 to 10 contain guidance on the requirements given in ISO 22301.

In this document, the following verbal forms are used:

a) "should" indicates a recommendation;

b) "may" indicates a permission;

c) "can" indicates a possibility or a capability.

0.6 Business continuity

Business continuity is the capability of the organization to continue delivery of products or services at acceptable predefined capacities following a disruption. Business continuity management is the process of implementing and maintaining business continuity (see 8.1.2 and Figure 5) in order to prevent loss and prepare for, mitigate and manage disruptions.

Establishing a BCMS enables the organization to control, evaluate and continually improve its business continuity.

In this document, 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.

Disruptions have the potential to interrupt the organization's entire operations and its ability to deliver products and services. However, implementing a BCMS before a disruption occurs, rather than responding in an unplanned manner after the incident, will enable the organization to resume operations before unacceptable levels of impact arise.

Business continuity management involves:

a) identifying the organization's products and services and the activities that deliver them;

b) analysing the impacts of not resuming the activities and the resources they depend on;

c) understanding the risk of disruption;

d) determining priorities, time frames, capacities and strategies for resuming the delivery of products and services;

e) having solutions and plans in place to resume the activities within the required time frames following a disruption;

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

The organization's approach to business continuity management and its documented information should be appropriate to its context (e.g. operating environment, complexity, needs, resources).

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

Activities can be 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 enables an organization to identify activities that are essential to it being able to meet its obligations. Through business continuity, an organization can recognize what is to be done to protect its resources (e.g. people, premises, technology, information), supply chain, interested parties and reputation before a disruption occurs. With that recognition, the organization can put in place a response structure, so that it can be confident of managing the impacts of a disruption.

Figure 2 and Figure 3 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.

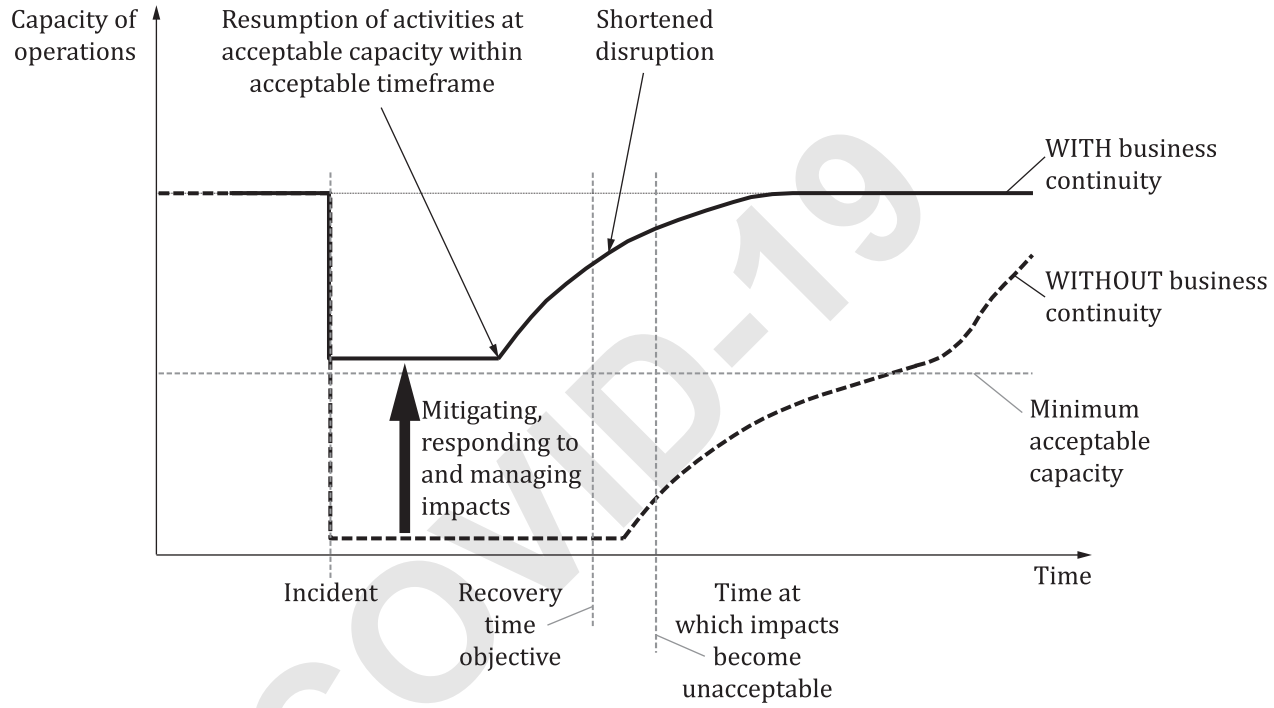

Figure 2 — Illustration of business continuity being effective for sudden disruption

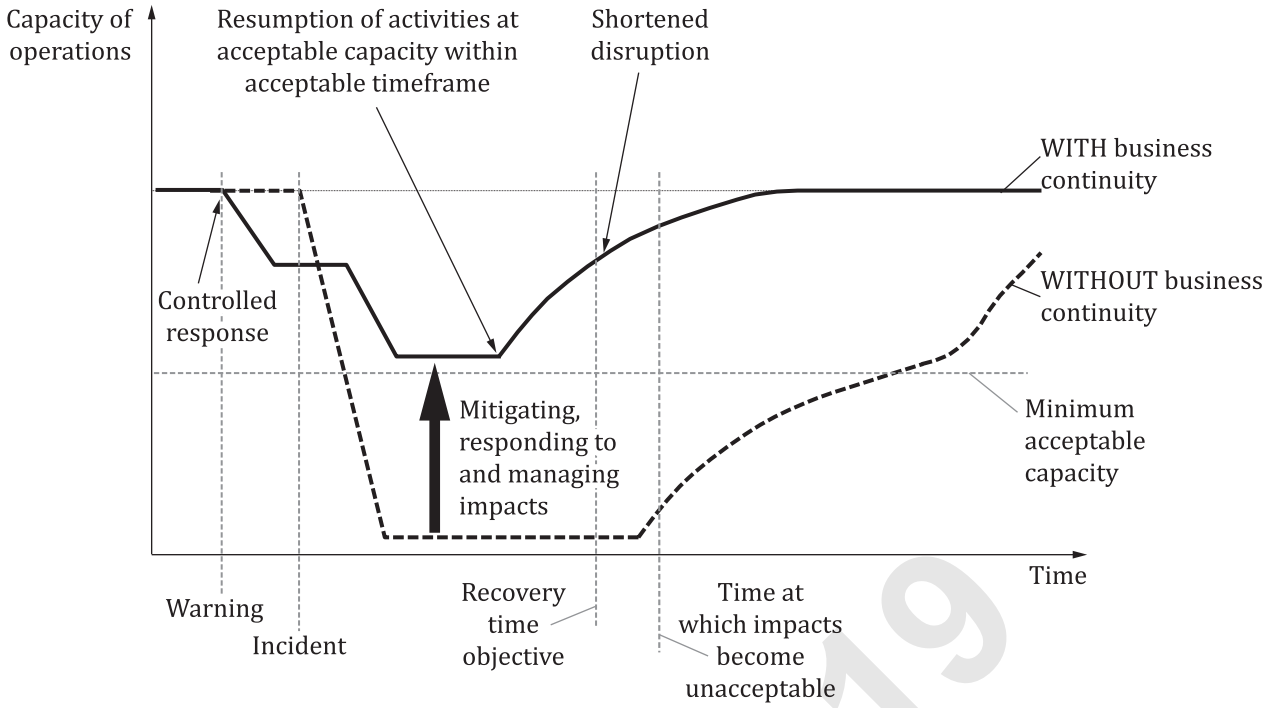

Figure 3 — Illustration of business continuity being effective for gradual disruption (e.g. approaching pandemic)

INTERNATIONAL STANDARD **ISO 22313:2020(E)**

Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301

1 Scope

This document gives guidance and recommendations for applying the requirements of the business continuity management system (BCMS) given in ISO 22301. The guidance and recommendations are based on good international practice.

This document is applicable to organizations that:

a) implement, maintain and improve a BCMS;

b) seek to ensure conformity with stated business continuity policy;

c) need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption;

d) seek to enhance their resilience through the effective application of the BCMS.

The guidance and recommendations are applicable to all sizes and types of organizations, including large, medium and small organizations operating in industrial, commercial, public and not-for-profit sectors. The approach adopted depends on the organization's operating environment and complexity.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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, *Security and resilience — Vocabulary*

ISO 22301, *Security and resilience — Business continuity management systems — Requirements*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
business continuity management
process of implementing and maintaining business continuity

4 Context of the organization

4.1 Understanding the organization and its context

This clause provides recommendations for understanding the context of the organization in relation to the BCMS. Recommendations for establishing and maintaining business continuity are addressed in 8.1.

The organization should evaluate and understand the external and internal issues (including positive and negative factors or conditions for consideration) that are relevant to its overall objectives, its products and services, and the amount and type of risk that it may or may not take. This information should be taken into account when implementing and maintaining the organization's BCMS and assigning priorities.

The organization's external context includes, where relevant, the following:

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

— social and cultural aspects;

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

— supply chain commitments and relationships (see also ISO/TS 22318);

— drivers (e.g. risk, technology) and trends having impact on the objectives and operation of the organization;

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

— communication channels, including social media, used for ascertaining and forming such relationships.

The organization's internal context includes, where relevant, the following:

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

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

— existing management systems;

— information and data (stored in physical or electronic form) and decision-making processes (formal and otherwise);

— interested parties within the organization, including internal suppliers [consideration of service level agreements (SLAs), assessed resiliency and recovery arrangements], see ISO/TS 22318;

— policies and objectives, and the business 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;

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

— internal communication channels used for the exchange of information within the workforce (e.g. social media).

4.2 Understanding the needs and expectations of interested parties

4.2.1 General

The organization owes a duty of care to a wide range of people within and outside the organization (see also ISO/TS 22330). When establishing its BCMS, the organization should ensure that the needs and requirements of all interested parties are taken into consideration.

The organization should identify all interested parties that are of relevance to its BCMS (see Figure 4) and, based on their needs and expectations, should determine their requirements. It is important to identify not only obligatory and stated requirements, but also any that are implied.

When planning and implementing the BCMS, it is important to identify actions that are appropriate in relation to interested parties but differentiate between them. For example, while it can be appropriate to communicate with all interested parties following a disruption, it may not be appropriate to communicate with all interested parties when implementing and maintaining business continuity management (see 8.1.2).

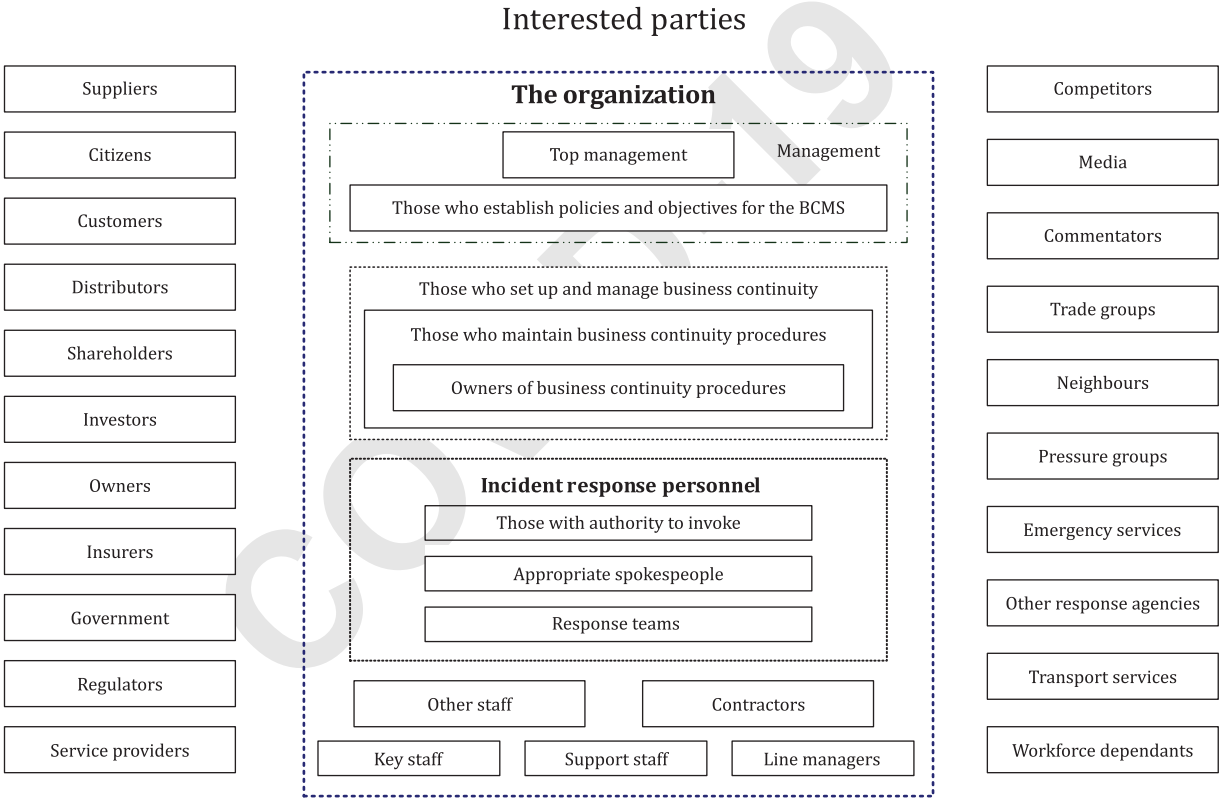

Figure 4 — Examples of interested parties in public and private sectors

4.2.2 Legal and regulatory requirements

The application of this document pre-supposes an awareness of the applicable legal and regulatory requirements.

Requirements can be implied, stated or obligatory. The information regarding these requirements should be documented and kept up to date. New requirements or changes to existing requirements should be communicated to affected employees and other interested parties.

The organization should show that it has access to current and pending legal and regulatory requirements that are relevant to its operations and how these requirements are met. Requirements can include:

a) incident response, including emergency management and other relevant legislation;

b) business continuity, which can dictate the scope of the programme or the extent or speed of recovery;

c) risk, requirements defining the scope or methods of risk management;

d) hazards (e.g. operating requirements relating to dangerous materials stored at the location).

Organizations operating in multiple locations may need to satisfy requirements of different jurisdictions.

4.3 Determining the scope of the business continuity management system

4.3.1 General

The purpose of determining the scope of the BCMS is to identify its boundaries and applicability to ensure coverage of all relevant products and services, activities, locations, resources, suppliers and other dependencies.

The scope should address the issues identified in 4.1, the requirements of interested parties determined in 4.2, and the organization's mission, goals and obligations.

The organization should prepare a statement that sets out the scope of the BCMS in a manner and in terms appropriate to the size, nature and complexity of the organization. The statement should be available to interested parties.

4.3.2 Scope of the business continuity management system

The organization should:

a) establish, by reference to products and services, the parts of the organization that are included within or excluded from the scope of the BCMS, for example:

   1) only including delivery of a specific product to a country or region;

   2) excluding a product that is no longer viable or is of low value to the organization;

   3) only including a sub-set of products and services;

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

The scope may:

— include an indication of the scale or magnitude of incident that the BCMS will address;

— identify how the BCMS fits into the organization's business strategy and approach to risk management.

4.3.3 Exclusions to scope

The scope determines the locations, products and services, activities and resources to which the BCMS applies. It follows that all dependencies will be in scope even if they have not been explicitly identified in the scope statement. For example, if a manufacturing company includes a product in its BCMS scope, then the supply of raw materials, processing, delivery and any support functions (such as data

processing, purchasing and human resources) at any location that are involved directly or indirectly in its delivery to the customer will be included.

Exclusions should not affect the organization's ability to meet business continuity requirements as determined by the business impact analysis (see 8.2.2). Activities, resources and supply chains that are required to deliver in-scope products and services cannot be excluded.

Exclusions from the scope of the BCMS should be documented and the justification for them explained.

If the BCMS is being integrated into an existing management system, the organization should ensure that all elements of the BCMS are included.

4.4 Business continuity management system

The purpose of this subclause is to emphasize the need for the organization to implement and maintain processes that will enable the BCMS to meet the requirements of ISO 22301, including interactions between the processes.

In determining the processes and their application throughout the organization, the organization should:

a) determine the inputs required and the outputs expected from these processes;

b) determine the sequence and interaction of these processes;

c) determine and apply the criteria and methods (including monitoring, measurements and related performance indicators) needed to ensure the effective operation and control of these processes;

d) determine the resources needed for these processes and ensure their availability;

e) assign the responsibilities and authorities for these processes;

f) address the risks and opportunities as determined in 6.1;

g) evaluate these processes and implement any changes needed to ensure that these processes achieve their intended results;

h) improve the processes and the BCMS.

To the extent necessary, the organization should:

— maintain documented information to support the operation of its processes;

— retain documented information to have confidence that the processes are being carried out as planned.

5 Leadership

5.1 Leadership and commitment

5.1.1 General

All levels of management throughout the organization should demonstrate leadership and commitment as applicable to their areas of responsibility.

5.1.2 Top management

Top management should demonstrate leadership and commitment by:

a) assigning managerial roles and ensuring they are fulfilled (see 5.1.3);

b) establishing business continuity policy (see 5.2);

c) appointing one or more persons with the appropriate authority and competencies to be responsible for the BCMS and accountable for its effective operation (see 5.3);

d) communicating the importance of business continuity and conforming to BCMS requirements;

e) making available the necessary resources, including appropriate levels of funding (see 7.1);

f) promoting continual improvement (see 10.2);

g) ensuring that the intended outcomes of the BCMS are achieved;

h) providing other levels of management with support that enables them to demonstrate the leadership and commitment applicable to their areas of responsibility.

5.1.3 Other managerial roles

Other managerial levels should demonstrate their leadership and commitment by:

a) establishing business continuity objectives that are compatible with the organization's strategic objectives (see 6.2);

b) integrating BCMS requirements into the organization's business processes (see 8.1);

c) displaying awareness of applicable legal, regulatory and other requirements (see 4.2.2);

d) establishing BCMS roles, responsibilities and competencies (see 5.3 and 7.2);

e) achieving the intended outcomes of the BCMS;

f) actively engaging in the exercise programme (see 8.5);

g) conducting internal BCMS audits (see 9.2);

h) conducting effective management reviews of the BCMS (see 9.3);

i) directing and supporting improvement of the BCMS (see 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.

5.2 Policy

5.2.1 Establishing the business continuity policy

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

a) is a concise, high-level statement of top management's intention and direction for the BCMS;

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

c) provides a framework for objective setting;

d) includes a clear commitment to satisfying applicable requirements, including legal and regulatory obligations;

e) includes commitment to continual improvement of the BCMS.

The policy should:

— specify the scope and boundaries of the organization's business continuity, including limitations and exclusions (see 4.3);

— identify any authorities and delegations required, including the person or persons responsible for the organization's BCMS (see 5.3);

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

The policy may contain the following:

— a funding commitment;

— references to other related policies;

— a requirement to implement business continuity;

— a commitment to exercise and maintain business continuity.

For organizations with existing management systems, it may be appropriate to integrate the BCMS policy with those relating to the other management systems.

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

5.2.2 Communicating the business continuity policy

The business continuity policy should:

a) be available and maintained as documented information;

b) be communicated, understood and applied within the organization;

c) be made available to interested parties as approved by management.

5.3 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 be responsible and accountable for the BCMS. Top management may appoint other bodies (e.g. a steering committee) to oversee the implementation and ongoing monitoring of the BCMS. Representatives, irrespective of their other responsibilities, should be appointed with defined roles, responsibilities and authority for:

— ensuring the BCMS conforms to the business continuity policy;

— reporting on the performance of the BCMS to top management for review and as the basis for improvement (see Clause 9 and 10);

— promoting awareness of business continuity throughout the organization (see 7.3);

— ensuring the effectiveness of procedures developed for responding to incidents (see 8.4.4.2.2).

The management representative may:

— be given a specific title (e.g. "business continuity manager", "business continuity officer" or "resilience manager");

— hold other responsibilities within the organization;

— be from any area of the organization.

Representatives from functions or locations of the organization may be identified to assist in the implementation of the BCMS (e.g. those responsible for risk-related matters). 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. Table 3 provides examples of BCMS roles and responsibilities that could be appropriate.

NOTE Examples of teams and possible roles and responsibilities that could be appropriate for responding to incidents and resuming activities are provided in see Table 5 (see 8.4.4).

Depending on the size of the organization, the roles and responsibilities set out in Table 3 could be set up in a different way. The important thing to ensure is that all responsibilities are part of a role and have an owner.

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

Table 3 — Examples of BCMS roles and responsibilities

Role	Responsibilities
Top management representative	— Be accountable for the BCMS — Represent business continuity management at management reviews
Business continuity manager	— Be responsible for the BCMS — Establish and demonstrate commitment to business continuity policy — Lead all programme activities and coordinate with other functions — Nominate team members with appropriate seniority, authority and competence — Facilitate the approval of solutions, procedures and exercise programmes — Put forward team recommendations at management review meetings
Business continuity management team	— Implement business continuity management across the organization — Maintain documentation — Ensure that reviews of the programme are conducted on a timely basis — Assess the adequacy of business continuity for individual functions — Organize and coordinate business continuity awareness programmes — Create exercise programmes and seek approval from the appropriate authority — Conduct exercise briefings and debriefings — Keep interested parties informed of the programme — Ensure that exercising takes place in accordance with the exercise programme — Ensure that internal audits and management reviews are carried out on time — Maintain relationships with functions and liaise with them during disruptions — Ensure that corrective action plans are implemented in a timely manner — Facilitate the efforts of functional representatives/coordinators

Table 3 *(continued)*

Role	Responsibilities
Functional representatives	— Maintain business continuity procedures — Inform the business continuity manager of the status of preparedness — Perform and report on programme activities as directed — Confirm that suppliers' continuity plans are tested and maintained — Coordinate the participation of personnel in exercises — Maintain records of business continuity exercises — Keep the team informed of changes that could affect business continuity — Follow up corrective actions in a timely manner — Keep the business continuity manager informed of progress on corrective actions

6 Planning

6.1 Actions to address risks and opportunities

NOTE The guidance in this subclause relates to the effectiveness of the BCMS. Guidance relating to risks of prioritized activities being disrupted is provided in 8.2.3.

6.1.1 Determining risks and opportunities

Determining and addressing risks and opportunities enables the organization to:

a) obtain assurance that the BCMS can achieve its intended outcomes;

b) prevent, or reduce, undesired effects;

c) achieve continual improvement.

The organization should determine actions to address the issues identified in 4.1, the needs and expectations of interested parties identified in 4.2, and the legal and regulatory requirements identified in 4.2.2.

This determination should include consideration of risks and opportunities and their potential impact on the effectiveness of the BCMS. Risks and opportunities can arise from:

— a lack of leadership and commitment from top management;

— insufficient funding of the BCMS leading to an ineffective response;

— poorly documented information;

— a lack of people with demonstrated competence;

— an inadequate management review process;

— an inability to break into new markets where business continuity is a requirement.

6.1.2 Addressing risks and opportunities

The organization should plan the actions needed address these risks and opportunities in a manner that:

— prevents unintended outcomes;

— takes advantage of any opportunities to improve the BCMS;

— achieves integration into the BCMS process (see 8.1);

— ensures that documented information will be available to evaluate if the actions have been effective (see 9.1).

6.2 Business continuity objectives and planning to achieve them

6.2.1 Establishing business continuity objectives

The organization should establish objectives for the implementation and maintenance of business continuity management (see Clause 8). These should be in line with organization's overall objectives, and should include identifying responsibilities and setting appropriate and realistic targets for completion. Planning should be communicated throughout the organization. Progress on its implementation should be monitored and documented.

As the BCMS evolves, this plan should be reviewed regularly and, where appropriate, updated.

6.2.2 Determining business continuity objectives

When determining its business continuity objectives, the organization should ensure that they specify clearly:

a) what will be done;

b) the resources that will be needed;

c) who will be responsible;

d) completion dates;

e) how results will be evaluated.

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

— "Top management will allocate the necessary resources to ensure that a BCMS, consistent with ISO 22301 is established by *date* for all products and services.";

— "Director A will engage with XXX Consultants to achieve certification against ISO 22301 by *date* for *named products and services*.";

— "Top management will use existing resources to ensure that, by *date*, we will have ISO 22301 compliant business continuity in place to meet our obligations to *named* customers.";

— "The IT Director will work with our vendors to shorten the recovery time of activities supporting *named products and services* by 10 %. This will be achieved by *date*.";

— "Without drawing on additional resources, the production manager will have in place, by *date*, business continuity management that meets the requirements of ISO 22301 and protects *named products and services*.".

6.3 Planning changes to the business continuity management system

Change management is an important consideration for all management processes.

Changes to the BCMS, including those identified in 10.1, should be carefully planned to ensure that the intended purpose is fully investigated and understood. This should include contemplation of the consequences of the changes proposed, ensuring that both anticipated and unintended consequences are considered, and making sure that the integrity of the BCMS is preserved.

The organization should also make sure that appropriate and sufficient resources are available, and that responsibilities and authorities are allocated or reallocated as necessary.

7 Support

7.1 Resources

7.1.1 General

The organization should determine and ensure availability of 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 BCMS matters, internally and externally;

d) provide for the on-going operation and continual improvement of the BCMS.

Resources should be available 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) systems, 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);

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.

7.2 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" and may include:

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

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

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

— performance evaluation;

— knowledge sharing;

— job sharing;

— hiring or contracting competent persons;

— training of target groups;

— the documentation and monitoring of training received;

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

— the improvement of the 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.

Types of training that may be appropriate for establishing, managing and maintaining the BCMS are as follows:

— setting up and managing business continuity management;

— conducting a business impact analysis;

— conducting a risk assessment;

— communication skills;

— project management;

— developing and implementing business continuity documentation;

— running an exercise programme.

Competence may be reinforced by any of the following:

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

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

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

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

The organization should 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

The organization should ensure that all persons working under its control (e.g. staff, contractors, suppliers) are aware of the business continuity policy and the organization's business continuity objectives, and:

— how to reduce the likelihood of disruptions and their role with regard to incident detection, mitigation, self-protection, evacuation, response, continuity and recovery;

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

— dependencies on suppliers and outsource partners and any associated risks to business objectives;

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

— their contribution to the effectiveness of the BCMS, including the benefits of improved business continuity;

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

The organization should build, promote and embed business continuity management within the culture of the organization so that:

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

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

An organization with business continuity management embedded in its culture will:

— develop business continuity more efficiently;

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

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

— minimize the likelihood and impact of disruptions.

Embedding business continuity management within the culture of the organization is supported by:

— the involvement of all personnel in the organization;

— a dispersed leadership across the organization;

— the assignment of responsibilities;

— measurement based on performance indicators;

— integrating business continuity into normal management practices;

— awareness raising;

— skills training;

— exercising business continuity plans.

An awareness programme may include:

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

— 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 business continuity management 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);

— regular communications with suppliers to ensure they understand the organization's business continuity requirements and can demonstrate their capability to meet agreed continuity capabilities.

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

— being a member of an industry interest group;

— being a member of a conference-organizing committee;

— delivering presentations at conferences and seminars;

— attending local or global business continuity conferences.

7.4 Communication

The organization should determine the communications relevant to the BCMS.

Communications relevant to the BCMS enable the organization to respond to the needs and expectations of interested parties (see 4.2). For communication to be effective, the organization should determine and, where appropriate, establish criteria for determining the following.

a) On what it will communicate: Communication regarding the BCMS can be needed depending on the nature of the organization and situation. Some organizations, for example, have legal or regulatory obligations to communicate.

b) When communication should take place: There can be thresholds beyond which it becomes imperative for the organization to communicate and the organization's context can dictate how frequently communication should take place.

c) With whom it will communicate: All interested parties will require communication from time to time, so it is important to determine for each interested party, the circumstances in which communication will be needed and the communication priorities.

d) The means of communication: Determining in advance the methods, tools and channels of communication, including alternatives, will enable the organization to communicate effectively.

e) The persons to execute the communication: The organization should identify spokespersons to represent the organization and designate specific people to be points of contact for communication.

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 (see 7.3) and when responding to an incident (see 8.4.4).

7.5 Documented information

7.5.1 General

Documented information required by ISO 22301 provides evidence of conformity to requirements and the 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 a suitable medium.

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

Documented information includes:

— understanding the organization and its context (see 4.1);

— legal and regulatory requirements (see 4.2.2);

— scope of the BCMS and any exclusions (see 4.3);

— policy (see 5.2);

— business continuity objectives and planning to achieve them (see 6.2);

— competence (see 7.2);

— business impact analysis and risk assessment (see 8.2);

— business continuity strategies and solutions (see 8.3);

— business continuity plans and procedures (see 8.4);

— exercise programme (see 8.5);

— monitoring, measurement, analysis and evaluation (see 9.1);

— internal audit (see 9.2);

— management review (see 9.3);

— nonconformity and corrective action (see 10.1).

In addition, documented information covering the following information can 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 solutions;

— 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 business continuity policy and plans, including evidence of risk monitoring of their suppliers, and evidence that their suppliers' continuity plans are maintained and exercised;

— contractor and supplier notification and response procedures;

— evidence of inspection, maintenance and calibration;

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

— BCMS review meeting minutes.

7.5.2 Creating and updating

To conform to the requirements for creating and updating documented information:

— all documented information should be clearly identifiable (e.g. name, reference number, description, date, author, version);

— the organization should specify the formats that are acceptable (e.g. language, software version, graphics) and the media that can be used for the storage of documented information (e.g. paper, electronic);

— the format and media used should be reviewed and approved for suitability and adequacy.

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;

— the competence of persons.

7.5.3 Control of documented information

7.5.3.1 Access to 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 or modified without appropriate authorization and from being accidentally deleted.

There are various access levels and combinations that may be granted (e.g. view only, view and change, restricted view). It can also be appropriate for the organization to classify its documented information according to its sensitivity (e.g. restricted, confidential, protected). Such classification can, for example, be needed for business continuity solutions relating to internal labour disruption, or where business continuity plans and procedures contain competitor-sensitive information.

7.5.3.2 Types of control

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

— distribute documented information;

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

— approve documents for adequacy prior to issue;

— review and update as necessary and to re-approve documents;

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

— ensure that relevant versions of all applicable documents are available at points of use;

— ensure that documents remain legible and readily identifiable;

— 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;

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

— establish document retention and archival parameters;

— 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 demonstrate awareness of all relevant legislation and regulations regarding the retention of documented information and should retain evidence of compliance.

8 Operation

8.1 Operational planning and control

8.1.1 General

The organization should determine, plan, implement and control the processes needed to establish and maintain business continuity management that meets applicable requirements (see Clause 4) and implement the actions determined in 6.1.

These processes should be integrated into the organization's business processes to ensure that they are managed appropriately and their effectiveness maintained.

The organization should establish control mechanisms that include:

a) deciding how these processes should be determined, planned, implemented and controlled (e.g. by establishing an implementation plan and agreeing a suitable methodology for implementing and maintaining business continuity management);

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

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.

The organization should ensure that outsourced processes and the supply chain are controlled (see 8.3.4.9)

8.1.2 Business continuity management

The elements of business continuity management, as shown in Figure 5, are as follows.

a) Operational planning and control (see 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 (see 8.2): Business impact analysis enables the organization to assess the impact that disruption of activities would have on delivery of its products and services. This enables the organization to prioritize the resumption of activities.

   Understanding the risks of disruption to these prioritized activities enables the organization to manage them.

   The outcome of business impact analysis and risk assessment enables the organization to determine appropriate parameters for its business continuity strategies and solutions.

c) Business continuity strategies and solutions (see 8.3): The identification and evaluation of a range of business continuity strategies enables the organization to identify solutions for reducing the risk and mitigating the impact of disrupting its prioritized activities and deal with any disruptions that occur. Selected business continuity solutions will provide for the resumption of deliveries of products and services at an acceptable capacity (production or service level) and within agreed time frames.

d) Business continuity plans and procedures (see 8.4): Business continuity plans and procedures enable the organization to manage a disruption and continue activities based on its business continuity requirements. There should be a defined response structure that identifies the teams responsible for responding to disruptions (see 8.4.2). The organization should establish and implement plans and procedures for warning and communication (see 8.4.3), responding to incidents (see 8.4.4.2.2), and recovery (return to business as usual) (see 8.4.5).

e) Exercise programme (see 8.5): An exercise programme enables the organization to validate the effectiveness of solutions, plans and procedures that have been put in place. An exercise programme also provides opportunities for the organization to:

   1) promote personnel awareness and competency development;

   2) ensure that its business continuity plans and procedures are complete, current and appropriate;

   3) improve its business continuity.

f) Evaluation of business continuity documentation and capabilities (see 8.6): The organization should evaluate its business continuity management to ensure that it is effective and enables the organization to achieve its business continuity objectives.

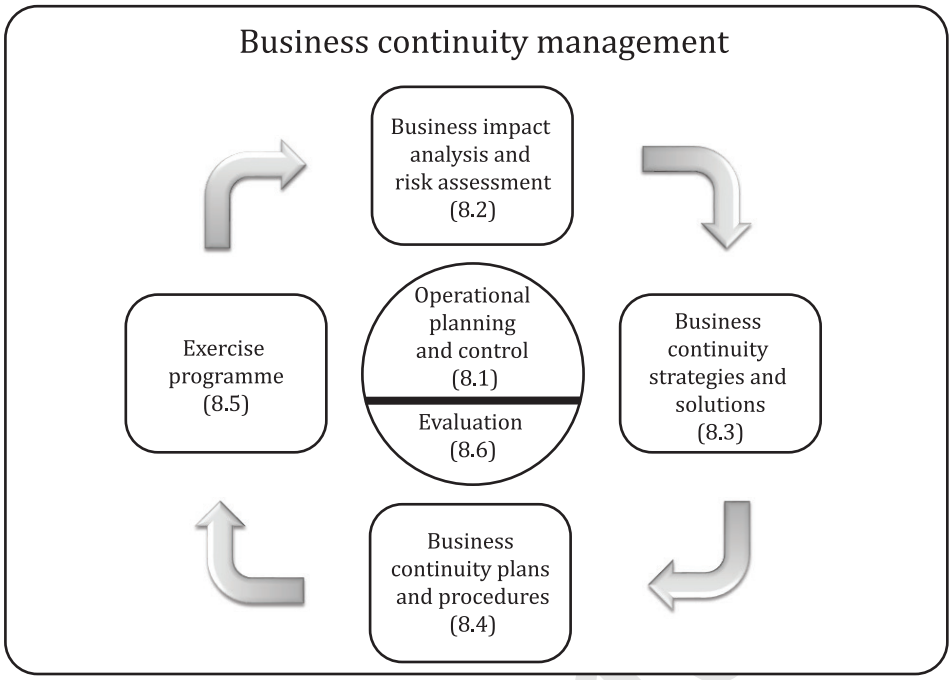

Figure 5 — Elements of business continuity management

8.1.3 Maintaining business continuity

Effective maintenance of business continuity includes:

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

— promoting and embedding business continuity management within the organization and other interested parties, where appropriate;

— managing costs associated with business continuity;

— establishing and monitoring change management and succession management regimes within the BCMS;

— arranging or providing appropriate staff training and awareness;

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

Each component of an organization's business continuity 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 business continuity management is effectively managed.

Techniques for ensuring that business continuity stays effective, include:

— implementing good practice;

— administering the exercise programme;

— coordinating the regular review and update of business continuity, including reviewing or reworking the analysis of business impacts and risk assessments;

— ensuring that business continuity procedures remain appropriate to the needs of response teams.

8.2 Business impact analysis and risk assessment

8.2.1 General

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 disrupting delivery of these products and services (and the activities that support them) would have on the organization and interested parties. 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.

The organization should implement and maintain processes that systematically analyse the business impacts (see 8.2.2) and assess the risks of disruption (see 8.2.3), the outcomes of which enable the organization to identify business continuity strategies and solutions (see 8.3). The analysis of business impacts and assessment of risks should be reviewed at planned intervals and when there are significant changes within the organization or the context in which it operates.

It is for the organization to determine the order in which the analysis of business impact and the assessment of risk are performed as long as the risks to its prioritized activities (see 8.2.3) are assessed.

8.2.2 Business impact analysis

An analysis of business impacts enables the organization to set priorities for resuming activities that have been disrupted. Its main purpose is to enable the organization to identify and classify as "prioritized" any activities that could need urgent action when they have been disrupted because failure to resume them quickly could result in unacceptable levels of adverse impact. It is possible that activities other than those needing to be recovered quickly will need to be prioritized. For example, an activity that does not need to be resumed for six months but would take a minimum of eight months to resume would need to be prioritized. Prioritized activities can therefore also be regarded as activities that can require business continuity solutions to be implemented before they are disrupted (see 8.3.5).

This document uses the term "prioritized activity" but organizations may use their own terms, time periods or orders of priority. Examples of terms include "critical", "essential", "vital" and "key". Examples of time periods include "0–2 hours", "0–1 day" and "1–3 days". Examples of priorities include "high", "medium" and "low", or "1st", "2nd" and "3rd".

Every organization describes how it operates in its own way. For example, an organization may describe activities as being tasks or sets of tasks that the organization performs in order to produce or deliver its products and services (see Figure 6). Other organizations may wish to describe products and services as being created by processes made up of activities.

The analysis should cover all activities within the scope of the BCMS. It is acceptable to perform the analysis on groups of activities, for example, relating to specific products and services (see Figure 6).

When conducting the analysis of business impacts, the terminology used should reflect the way the organization describes its own operations.

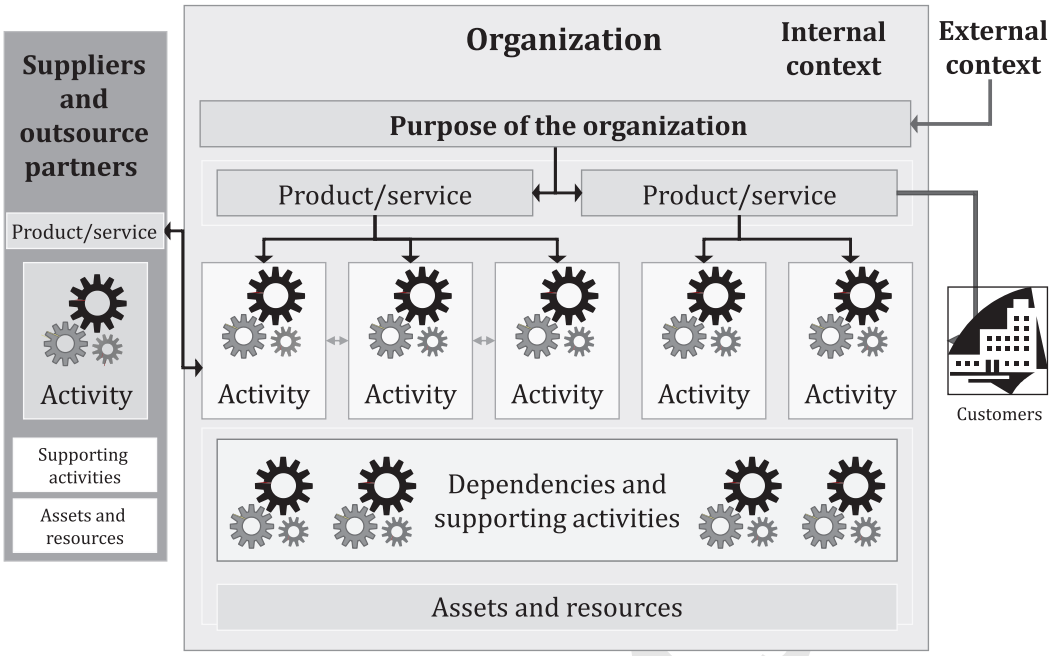

Figure 6 — Understanding the organization

ISO/TS 22317 contains further guidance on conducting a business impact analysis. It is a Technical Specification that presents a phased approach as a way of meeting the requirements of ISO 22301.

The analysis of business impacts enables the organization to determine the adverse impacts that disruptions would have on its operations and prepare, as an outcome, a statement and a justification of business continuity requirements.

The analysis also enables the organization to:

— obtain an understanding of its products and services and the activities that deliver them;

— determine priorities and time frames for resuming delivery of products and services;

— identify the resources that could be required for continuity and recovery;

— identify dependencies (both internal and external).

The process for analysing business impacts should be used to determine business continuity priorities and requirements.

The process should include defining evaluation criteria for the analysis of business impact, including the types of impact and time frames to be considered. Both should be based on the context, business objectives and aims of the organization and should consider the needs of interested parties. The evaluation criteria should be reviewed regularly, and more frequently during periods of change.

Types of impact (which may be referred to as “impact categories”) can include, for example, those shown in Table 4.

Table 4 — Examples of type of impact

Type	Description
Financial	Losses due to fines, penalties, lost profits, or diminished market share
Reputational	Negative opinion or brand damage
Operational	Extent and duration of disruption to flow of business operations
Legal and regulatory	Litigation liability and withdrawal of licence to trade
Contractual	Breach of contracts or obligations between organizations
Business objectives	Failure to deliver on objectives or take advantage of opportunities

The time taken for impacts to become unacceptable can vary between seconds and several months. The time frames will depend on the time-sensitivity of the organization's products and services. For example, to accommodate products that are very time sensitive, the time frames may need to be minutes or hours. Longer time frames would be appropriate for organizations with less time-sensitive products and services.

Disruption of activities can cause delivery of products and services to be impacted indirectly. For example, the loss of the ability to pay suppliers can damage the reputation of the organization and result in suppliers refusing to supply goods, which then prevents products being manufactured or services being delivered. Products and services also have daily variations in demand 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. Taking indirect consequences into account and making the assumption that disruption occurs at the worst time ensures that the maximum possible impacts are assessed.

It is for the organization's top management to determine the thresholds of impact that are unacceptable to the organization. The time it would take for impacts to become unacceptable can be referred to as "maximum tolerable period of disruption (MTPD)", "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)".

The business impact analysis should also include identifying dependencies of prioritized activities, which will enable the organization to ensure that they are included in the risk assessment (see 8.2.3) and available for determination of business continuity strategy and solutions (see 8.3).

The organization should be wary of determining resource requirements of prioritized activities (see 8.3.4) before selecting continuity solutions (see 8.3.3) because the dependencies of prioritized activities may not be relevant to the continuity solutions that are selected.

The process for analysing business impacts should include:

a) defining evaluation criteria relevant to the organization's context, including:

   1) types of impact;

   2) time frames;

b) identifying activities that support the delivery of the organization's products and services;

c) using the evaluation criteria to assess the anticipated impacts over time resulting from disruption of these activities;

d) estimating the time within which the impacts of not resuming activities would become unacceptable;

e) setting time frames within the time identified in d) above for resuming activities at specified minimum acceptable capacities (see Figures 2 and 3);

f) identifying prioritized activities;

g) identifying the dependencies of prioritized activities, including people (see 8.3.4.2), information and data (see 8.3.4.3), buildings, workplaces and associated utilities (see 8.3.4.4), equipment and consumables (see 8.3.4.5), ICT systems (see 8.3.4.6), transportation and logistics (see 8.3.4.7), finance (see 8.3.4.8), and partners and the supply chain (see 8.3.4.9);

h) identifying interdependencies of prioritized activities (e.g. procurement is dependent on finance to release funds).

In this document, the time frame for resuming an activity [see e) above] is referred to as the activity's "recovery time objective (RTO)". Setting an activity's RTO may also need to take into account:

— dependencies on related activities;

— the complexity of the recovery process.

It may be appropriate for organizations with complex recovery processes to set multiple RTOs for a range of acceptable capacities.

When considering the dependency of activities on information and data, the organization should ensure that information and data required for an activity to be resumed will be appropriately current. The organization may use the term "recovery point objective (RPO)" to achieve this. The RPO is the point up to which information and data used by an activity is restored to enable the activity to operate upon resumption. The RPO can also be used to determine the frequency of backup needed to avoid unacceptable loss of data and information, and other work-in-progress that could prevent an activity from being resumed.

ISO/IEC 27031 provides further guidance with regard to ensuring the currency of electronically held data. ISO/IEC 27002 provides guidance on ensuring the ongoing confidentiality, integrity and availability of data.

The analysis of business impacts should be documented including:

— the identification of legal, regulatory, and contractual requirements (obligations) and their effect on business continuity requirements (see 4.2.2);

— the endorsement or modification of the scope of the organization's BCMS (see 4.3);

— the evaluation of impacts on the organization over time as justification for business continuity requirements (time and capability);

— the identification of the relationships between products and services, activities and resources;

— the identification of supporting resources that are depended on by prioritized activities;

— the identification of dependencies on other activities, supply chains, partners and other interested parties.

Information may come from:

— interviews;

— questionnaires;

— workshops;

— other internal and external sources.

8.2.3 Risk assessment

NOTE The guidance in this subclause relates to the risks of prioritized activities being disrupted. Guidance relating to the effectiveness of the BCMS is provided in 6.1.

The purpose of the risk assessment is to enable the organization to assess the risks of prioritized activities being disrupted so that it can take appropriate action to address these risks.

The organization should implement and maintain 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 is a structured process for analysing risk in terms of likelihood and consequences before deciding on further treatment that could be required. This structured process attempts to answer some fundamental questions, such as the following.

— What could happen?

— What is the likelihood of it or them happening?

— What could be the consequences?

— Is there anything that could mitigate the consequences or reduce the likelihood?

The process should take into consideration the context of the organization and the needs and expectations of interested parties (see 4.1 and 4.2).

The organization should understand the threats and vulnerabilities relevant to the resources required by the organization's activities, particularly those:

— resources required by activities identified as high priority;

— where the replacement lead time for the resource is longer than the activity's recovery time objective.

The organization should select an appropriate method for identifying, analysing and evaluating risks that could lead to a disruption. ISO 31000 sets out the principles of risk management and associated guidelines. Typical elements that should be included in the context of this document are as follows.

a) Identification of risks: Potential sources of risk to the organization's prioritized activities and the processes, systems, data, people, assets, suppliers and other resources that support them. These can come from:

   1) specific threats that could at some point disrupt activities and resources (e.g. fire, flood, power failure, staff loss, staff absenteeism, computer viruses, hardware failure);

   2) disruptions, which could arise from vulnerabilities within resources (e.g. single points of failure, inadequacies in fire protection, lack of electrical resilience, inadequate staffing levels, poor IT security and resilience).

b) Analysis of risks: An understanding of the risk so that it can be evaluated and the most appropriate treatment can be determined. This should involve:

   1) considering the causes and sources of risk, the likelihood of both positive and negative consequences, and the effect that other factors could have on the likelihood;

   2) determining the risks, based primarily on their likelihood and anticipated consequences, but also taking into account the effectiveness and efficiency of existing controls.

   A key parameter in the analysis is likelihood, so confidence in its validity (based on divergence of opinion among experts, uncertainty, availability, quality, quantity and ongoing relevance of information, or limitations on modelling) should be considered and brought to the attention of decision makers and other interested parties.

   The analysis can be qualitative, semi-quantitative or quantitative.

c) Evaluation of risks: An evaluation of which disruption-related risks require treatment. This should focus on the resources required by activities with high priority or with significant replacement lead time.

The organization should be aware of any financial, regulatory/legislative or governmental obligations requiring the communication of these findings. In addition, certain societal needs can also warrant sharing of this information at an appropriate level of detail.

8.3 Business continuity strategies and solutions

8.3.1 General

Business continuity strategies are possible ways for the organization to meet its business continuity requirements.

— Business continuity strategies should be comprised of at least one business continuity solution but may require more than one solution to meet business continuity requirements.

— Business continuity solutions include approaches, arrangements, methods, procedures, treatments and actions that can be put in place to implement business strategies. Solutions can be used for more than one strategy.

Business continuity strategies and solutions:

a) enable the organization to resume business operations within the required time frames and at an acceptable capacity;

b) identify capabilities that the organization can implement and improve over time to mitigate disruption-related risks.

The identification of business continuity strategies and the selection of business continuity solutions should be based on the business impact analysis (see 8.2.2) and the risk assessment (see 8.2.3), taking into consideration the associated costs.

The organization should have in place procedures for identifying and selecting business continuity strategies and solutions, including review and approval of recommended solutions. The organization should consider options that can be implemented before, during and after a disruption.

8.3.2 Identification of strategies and solutions

8.3.2.1 General

Most strategies require one or more solutions but, for some of the organization's activities, doing nothing or deferring resumption may be acceptable strategies.

For example, a relocation strategy for resuming activities can be made up of a number of solutions including "emergency transport", "network redirection" and "alternate staffing". These solutions can also form part of the strategy "extending working hours".

Similarly, a production strategy for protecting prioritized activities can, for example, be made up of a number of solutions including "moving the manufacture of 30 % of Product A from Location A to Location B" or "splitting the manufacture of Product A between Location C and Location D".

To ensure that the operation of business continuity plans (see 8.4.4) is not adversely affected by the disruption, the organization may need to take precautions, for example, separating teams and recovered ICT systems across multiple locations. Total separation for all scales and types of disruption is not always achievable and it may be necessary to identify limitations and agree them with top management. Limitations can be expressed in terms of distance, minimum personnel or severity, and can be influenced by the response of public agencies to severe or widespread disruptions.

The organization should identify appropriate strategies and solutions 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 determining and selecting business continuity strategies and solutions, including the approval and implementation of recommended solutions (see 8.3).

ISO/TS 22331 provides further guidance on the determination and selection of business continuity strategies and solutions.

8.3.2.2 Protecting prioritized activities

Protection of prioritized activities may be achieved by:

— reducing the risk of the activities being impacted by a disruption;

— transferring activities to a third party (though the responsibility remains with the organization).

Alternatively, it can be possible to change how activities are performed if viable alternatives are available.

When identifying strategies and solutions for protecting prioritized activities, the organization should consider:

— the perceived vulnerability of the activity and the impacts that would arise if the activity were to stop;

— the cost of measures compared to the anticipated benefits;

— the urgency of the activity, since there will be less time to resolve the issue;

— their overall feasibility and suitability.

8.3.2.3 Stabilizing, continuing, resuming and recovering prioritized activities

Setting RTOs for resuming prioritized activities at agreed capacity enables the organization to identify strategies to shorten the period of interruption, reduce impacts and enable the timely recovery of prioritized activities.

To ensure that prioritized activities can be resumed within their RTOs, compatible RTOs should also be set for the dependencies and supporting resources. Organizations should also determine the capacities at which dependencies and supporting resources would need to be resumed. When setting these RTOs, the organization may need to consider:

— the possibility of providing a different service until the point when full resumption is required;

— ensuring that people are mobilized effectively;

— providing encouragement and support for people returning to work at time of need;

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

— backlogs and time needed to recover lost information;

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

Business continuity strategies may include the following.

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. When determining locations at which to resume an activity, damaged/affected sites and undamaged alternate sites should be considered.

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) Temporary workaround: Some activities may adopt a different way of working that 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 business as usual.

Examples of strategies include:

— providing spare manufacturing capacity at an alternate location;

— providing remote working capabilities for key staff.

8.3.2.4 Mitigating, responding to and managing impacts

Strategies for mitigating, responding to and managing the impacts of a disruption may include the following.

a) Insurance: The purchase of insurance can provide some financial recompense for some losses but will not meet all costs (e.g. uninsured perils, brand, reputation, interested parties value, market share, 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 other solutions.

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

c) Reputation management: Developing an effective warning and communication capability (see 8.4.3) and establishing effective incident communications procedures (see 8.4.4.5).

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 a disruption.

If there is a specific hazard over which the organization has no control and which could significantly disrupt the organization (e.g. earthquake or flooding), the organization should, where appropriate:

— identify strategies and implement solutions for limiting its potential impact;

— identify the external body responsible for monitoring the hazard;

— contact the external body to understand its notification protocols;

— analyse the notification protocols to determine if they align with the needs of the organization.

8.3.3 Selection of strategies and solutions

The selection of business continuity strategies should be based on the extent to which they:

a) enable prioritized activities to be resumed at agreed capacity within time frames identified during the business impact analysis (see 8.2.2);

b) are in line with the amount and type of risk that the organization may or may not take;

c) deliver benefits at manageable and reasonable cost.

The organization should re-examine all solutions when changes are made to the operation of the organization.

Business continuity solutions 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 solutions 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 4.3.3.

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 ongoing BCMS performance evaluation (see Clause 9). Accepting the risk can also require the affected products or services to be removed from the scope of the BCMS.

8.3.4 Resource requirements

8.3.4.1 General

The organization should determine the resource requirements to implement selected solutions.

The organization should establish:

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

— logistical capabilities and procedures to locate, acquire, store, distribute, maintain, test and account for services, personnel, resources, materials and facilities produced or donated;

— financial, logistical and administrative procedures to support the business continuity arrangements before, during and after an incident; these procedures should:

  — ensure that financial decisions can be expedited;

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

— 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;

— procedures for interested party assistance, communications, strategic alliances and reciprocal or mutual aid.

8.3.4.2 People

8.3.4.2.1 General

The organization should have people with the competency to respond to and manage incidents, and participate in the resumption of prioritized activities.

8.3.4.2.2 Incident response

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 disruption that significantly impacts or has the potential to significantly impact the organization.

Personnel may be assigned to teams according to their demonstrated competence in, for example:

— incident/strategic management (see 8.4.4.4);

— communications (see 8.4.4.5);

— safety and welfare (see 8.4.4.6);

— salvage and security (see 8.4.4.7);

— resuming activities (see 8.4.4.8);

— recovery of ICT systems (see 8.4.4.9).

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

Training appropriate for incident response and business recovery personnel includes:

— incident assessment;

— evacuation and shelter in place management, if applicable to the scope;

— arrangements at alternate worksites;

— techniques for handling internal and external communications effectively;

— dealing with people aspects (see ISO/TS 22330).

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 and new members should be trained when they join the response structure. These teams should also receive training on prevention of incidents that could escalate into crises.

8.3.4.2.3 Resumption of activities

The organization should identify appropriate measures to maintain and widen the availability of core skills and knowledge to enable activities to be resumed with reduced staff availability. People may not respond as expected during an incident and may need encouragement, reassurance and support. Employees, contractors and other interested parties who possess extensive specialist skills and knowledge should all be included. Techniques to protect or enhance these skills may include:

— a list of back-up skilled specialists and a 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;

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

Procedures that rely on the relocation of staff after an incident may need to consider:

— transportation of staff to another location;

— staff needs at the alternate site, such as:

  — accommodation;

  — catering facilities;

  — personal and family commitments;

  — training on different equipment;

  — challenges posed by home working.

Specialist roles may include:

— security;

— transportation logistics;

— welfare and emergency.

To encourage and reassure people who will be required to respond to a disruption, the organization should provide, for example, practical advice, risk awareness training, transport solutions and family-related support.

ISO/TS 22330 provides further guidance on the people aspects of business continuity.

8.3.4.3 Information and data

The words "information" and "data" are used interchangeably in everyday use. This document uses "information" to mean data that has been processed, organized and correlated to produce meaning. Information is therefore created from data, which includes, for example, facts, statistics and numbers held manually and in an electronic form that can be stored and used on a computer.

It is possible for information to be recreated from data during a disruption, but the processing time to do so can be very long and the means to do so may also not be available. Organizations should therefore consider activities' requirements for both information and data. If information or data required by an activity (not just a prioritized activity) is/are irretrievably lost, it could be impossible for the activity to be resumed.

Information and data vital to the organization's operation should be protected and recoverable according to the time frames identified during the business impact analysis. When determining the arrangements for storage and recovery of data, the organization should be aware of applicable legal requirements.

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

— confidentiality (e.g. if the activity is moved to another location);

— integrity: that information and data are reliable and can be trusted;

— availability: that information and data are available as quickly as the activity requires it (i.e. within the activity's RTO); information and data required during the response can be required immediately while other information and data may not be required until after the incident;

— currency: as up to date as required enabling the activity to operate (see 8.2.2), though information lost due to the incident may need to be recreated and data may need to be restored.

Where information and data are copied, various methods may be used, including virtual (electronic) formats (e.g. disk, cloud, tape) and physical (hardcopy) formats (e.g. microfiche, photocopies, creating dual copies at the time of production).

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

If copied information or data is/are stored too near to the original, the disruption could compromise the integrity or prevent access to it. However, a long distance can prevent information/data from being available when needed. It would be appropriate to have written evidence as to how these conflicting concerns have been resolved.

Information and data referred to in this subclause may include:

— contact information;

— supplier, interested parties and interested party details;

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

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

— metadata (i.e. information to describe audio-visual content and data essence in a defined format);

— notification and alert messages disseminated as an incident response measure;

— guidelines and criteria regarding who has the authority to invoke procedures.

8.3.4.4 Buildings, workplaces and associated utilities

Worksite solutions can vary significantly and a range of options can be available. Different types of incidents or threats could 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 solution that reduces the impact of the unavailability of its normal worksite(s). This may include one or more of the following:

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

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

— command centres;

— alternative premises provided by third-party specialists;

— working from home or at remote sites;

— other agreed suitable premises;

— use of an alternative workforce in an established site.

Alternative premises should be carefully selected by taking account of a geographical area that could be affected by the same incident. An incident such as a natural disaster can 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, due consideration should be given to:

— making sure that the premises are not so close that they are likely to be affected by the same incident;

— making sure that the premises are close enough that staff are willing and able to travel there;

— possible difficulties that could be caused by the incident.

The use of alternative premises for continuity purposes should 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 should be developed and documented.

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

8.3.4.5 Equipment and consumables

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

Some facilities and machinery can 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, can 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 that has supplies;

— identification of alternative/substitute supplies;

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

Where activities are dependent upon specialist supplies, the organization should identify the suppliers on which the prioritized activities depend, especially where there is a single source of supply. Solutions to manage the 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 suppliers;

— 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.

8.3.4.6 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 workarounds while its ICT systems 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;

— external services to which the organization subscribes.

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

— spreading them geographically (e.g. maintaining the same technology at different locations that will not be affected by the same disruption);

— holding older equipment as emergency replacement or spares;

— 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. Attention should therefore be given to:

— the location of technology sites and the distance between them;

— distributing technology across 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 reinstate ICT systems;

— accommodating the obsolescence of ICT systems.

If an organization hosts its ICT systems at more than one site, there could be an opportunity to implement a solution whereby each site is sized to accommodate the combined ICT systems 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 systems by making special provisions for replacement or restoration.

ISO/IEC 27031 provides further guidance on ICT readiness for business continuity.

8.3.4.7 Transportation and logistics

Transportation may need to be provided after an incident for:

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

— staff relocated to an alternative work location;

— resources needed at a different location.

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

— identifying possible scenarios of logistic disruptions, including those caused directly by an incident or unusual situation;

— securing alternative means of transportation and routes to deal with unusual traffic conditions;

— agreements with alternative transport providers.

8.3.4.8 Finance

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

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

— reimbursement of staff expenses;

— major expenditures on, for example, the 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 the formal recording of expenses during and following a disruption.

8.3.4.9 Partners and the supply chain

Business networks and supply chains are often broad, complex and interdependent, with multiple tiers. It is essential to understand the supply chain and the risks it poses to the organization. When analysing business impacts (see 8.2.2), the organization should undertake, jointly with relevant suppliers, an analysis of supply chains on which prioritized activities depend. Suppliers, in turn, should be required to cascade the analysis to their suppliers.

The supply chain analysis should be based on a set of criteria developed by the organization, giving a common organizational approach to assess the level of dependency on the supply chain and specific suppliers within it and to understand the timescales of finding alternative arrangements.

Techniques for obtaining assurance and evaluating suppliers' and partners' business continuity may include:

— specifying business continuity requirements in tenders and contracts;

— periodic auditing of supplier plans;

— reviewing exercise and maintenance programmes;

— participating in joint business continuity exercises.

If a product, service or activity has been outsourced, the accountability for that product, service or activity remains with the organization.

Where prioritized activities or business continuity solutions rely on products and services from a supplier, the organization should evaluate the suppliers' business continuity to obtain assurance that the supplier has effective business continuity arrangements in place for these products and services, for example, by examining the results of exercises.

The organization may wish to concentrate its efforts on suppliers whose failure to deliver products and services would disrupt prioritized activities most quickly.

8.3.5 Implementation of solutions

Selected solutions should be implemented and maintained over time.

Following the selection of business continuity solutions, management should be involved in selecting business continuity resources (e.g. workspace, people, equipment, supplies). Care should be taken to ensure these resources will be available at the time of the incident.

To ensure that resumption and mitigation strategies are achievable, the organization should define and implement all solutions that need to be in place before a disruption. If the lead time for activating a solution exceeds business continuity requirements, the organization should implement the selected solution in advance of the disruption.

8.4 Business continuity plans and procedures

8.4.1 General

The organization should have a response structure supported by business continuity plans and procedures for:

— controlling the response to the disruption;

— communicating effectively with interested parties;

— utilizing business continuity solutions to resume activities within their RTOs.

A plan comprises one or more procedures. Collectively, plans and procedures should:

— identify the immediate steps to be taken and assist with timely decision-making;

— be sufficiently flexible to accommodate unanticipated threats and changeable situations;

— focus on the anticipated impacts of disruptions;

— align with the business continuity solutions selected by the organization to minimize impacts;

— clearly identify roles and assign responsibilities for all tasks to be undertaken.

8.4.2 Response structure

8.4.2.1 Purpose

An effective response structure enables organizations to detect events, identify incidents and determine whether or not they are likely to lead to disruption. The organization should develop an incident response structure that will provide an effective response to disruptions, regardless of cause. If there is no agreed and documented structure in place, it is likely that the organization will be incapable of responding effectively to disruption and will not be able to resume disrupted activities within the necessary time frames.

8.4.2.2 Design

The incident response structure should clearly identify:

— the teams responsible for responding to incidents and resuming activities;

— the team hierarchy;

— the roles and responsibilities of the teams.

The response structure should be simple and capable of being formed quickly. It should also provide mechanisms that ensure the timely communication of information and decisions.

There is no single incident response structure that is suitable for all organizations. Each organization should design its own structure, considering the following:

— the existing management structure;

— the organization's nature, culture, scale, complexity and process infrastructure;

— the business continuity solutions selected;

— the organization's business continuity requirements;

— any perceived threats to the organization.

Larger or complex organizations may need to establish separate teams to focus on different aspects of the incident. In smaller organizations, it can be feasible for one team to handle an incident, but it should never be the responsibility of a single individual.

8.4.2.3 Team capabilities

Collectively, the teams should be capable of:

— assessing the nature and extent of the disruption and its potential impact;

— measuring the potential impacts of the incident against predefined impact thresholds in order to determine whether or not a formal response is justified;

— initiating an appropriate response to a disruption, activating plans, mobilizing response teams and ensuring the availability of required resources;

— planning all actions to be undertaken;

— establishing priorities for all actions, giving first priority to life safety;

— monitoring how the incident unfolds and the effectiveness of the organization's response in dealing with impacts and consequences;

— activating suitable business continuity solutions;

— providing an effective command and control of the organization's response to the incident and responding to changes as the situation evolves;

— communicating with interested parties including, in particular, the workforce, affected family members, visitors, authorities and the media.

8.4.2.4 Team composition and guidance

Each team should have:

a) identified team members and alternates who have the necessary responsibility, authority and competence to enable the team to fulfil its role and responsibilities;

b) documented procedures for guiding the team's actions (see 8.4.4).

8.4.3 Warning and communication

8.4.3.1 General

Handling initial communications effectively from the outset of a disruption can make a huge difference to the effectiveness of the organization's response. Effective communication can only be achieved if the organization is clear on what, when, with whom and how to communicate. The organization should therefore establish documented procedures for the following warning and communication-related actions and identify who will be responsible for performing them:

— internal communication between different levels and functions within the organization, including within the response structure;

— alerting interested parties and receiving, documenting and responding to communications from them (this can include emergency contacts of employees);

— ensuring that communication equipment and facilities are available;

— facilitating structured communication with emergency responders;

— managing the organization's response to the media and ensuring that it aligns with the organization's communications strategy;

— recording vital information about the incident, actions performed and decisions taken.

The organization should ensure that effective procedures and facilities are in place for receiving, documenting and responding to warnings, alerts and external communications from national or regional risk advisory systems or equivalent. Some organizations may need to establish dedicated or ad hoc facilities located sufficiently far from the affected site that their operation will not be impeded by the incident. Special arrangements can be required for those with specific needs (e.g. the elderly and those with disabilities). For guidance on the dissemination of warnings, including information content and communication channels, refer to ISO 22322.

Communications equipment can be affected by disruptions, so a variety of alternatives may need to be available, for example:

— loud-hailers;

— public address systems;

— spare mobile phones;

— satellite phones;

— two-way radios.

8.4.3.2 Alerting interested parties

In some circumstances, interested parties can be impacted by a disruption that has already started or is imminent. For example, disruptions at an organization that undertakes hazardous operations or stores toxic products could result in the organization's neighbours being put in danger. Such organizations should consider:

— establishing procedures that would enable hazards to be monitored;

— determining in advance public warning information that they may need to provide during a disruption;

— identifying geographical areas to which public warning information may need to be sent;

— evaluating scientifically potential levels of seriousness of hazards;

— defining scientifically based criteria for issuing warnings and ensuring that there are procedures in place for transferring warning information to organizations with public warning responsibilities;

— establishing relationships with external bodies responsible for potentially affected areas.

It can also be necessary for such organizations to:

— establish a relationship with an external organization with public warning responsibilities;

— make sure that their neighbours understand how alarms are issued and how to respond.

Warning and communications procedures should be exercised as part of the organization's exercise programme (see 8.5).

8.4.4 Business continuity plans

8.4.4.1 General

Business continuity plans set out how teams will respond to disruptions and resume activities within the scope of the BCMS.

Because terminology differs between organizations and, in many instances, specific terms are used interchangeably, it is essential that the roles and responsibilities of teams are clearly stated, and the documented procedures supporting them clearly state their purpose, scope and objectives (see Table 5).

Table 5 — Examples of teams and possible roles and responsibilities

Team	Role	Responsibilities
Site emergency response Facilities management Security	Emergency response	Life safety Damage limitation
Damage assessment	Damage assessment	Damage assessment
Incident management	Incident management and control	Incident management
Crisis management Senior management	Strategic decision-making Communication during incident	Strategic management Crisis management Communications Public relations
Communications	Communication during incident	Communications Public relations
ICT recovery	Recovering ICT systems and infrastructure	ICT disaster recovery NOTE Guidance on ICT procedures can be found in ISO/IEC 27031.
Finance Administrative	General and financial administration	Finance and administration
Human resources Occupational health	Welfare and special needs Interested party well-being	Human resources Safety and welfare
Salvage Security Facilities ICT	Salvage of facilities, ICT systems and data Security	Salvage and security
Business continuity	Resume disrupted activities	Coordinate resumption Manage resources

8.4.4.2 Coverage

8.4.4.2.1 General

Collectively, business continuity plans should address all aspects of responding to an incident and should be specific to the teams that will use them. It may therefore be beneficial to:

— involve a wide range of personnel, including specialist teams, in the development of business continuity plans;

— use feedback from exercising and draw on lessons learned from disruptions.

Timescales and performance levels should be based on the information gathered during the business impact analysis (see 8.2.2) and the selection of business continuity strategies and solutions (see 8.3.3).

8.4.4.2.2 Responding to incidents

When dealing with an incident, there are number of actions that may need to be considered. These should be included in documented procedures and include:

a) responding to and assessing the incident, including:
   1) determining what happened and how it occurred;
   2) identifying which the parts of the organization and interested parties have been or could have been affected;
   3) trying to anticipate the duration of the incident and the likely impacts;
   4) assessing whether the incident will be managed by routine management arrangements;
   5) judging by reference to pre-defined thresholds whether the incident could lead to disruption;
b) managing the immediate consequences of the incident, giving due regard to the welfare issues of affected persons (including team members) and impacts on the environment, considering options for responding to the incident, and preventing further loss or damage;
c) evaluating the incident assessment against activation criteria for each of the procedures;
d) declaring an incident and activating the procedures when activation criteria have been met;
e) mobilizing the incident response personnel in teams for stabilization, continuity and recovery activities;
f) establishing a central location for use by the team managing and controlling the incident (command centre);
g) prioritizing issues and activities to be undertaken in managing the incident and its impacts;
h) controlling and coordinating all activated procedures;
i) activating or establishing alternate sites for the restoration of IT or other infrastructure capability and for the temporary operation of the organization's activities;
j) monitoring the incident as it progresses;
k) reviewing and adapting plans in response to changing circumstances;
l) de-escalating, standing down and returning to routine operations as sustainable capability is re-established;
m) conducting a debrief and identifying learning opportunities;
n) ensuring good governance and the 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 RTO of the activity that supports that product or service;
— be sufficiently reliable.

This may be achieved by:

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

— contracts, agreements or service levels with third parties.

8.4.4.3 Content and usability

8.4.4.3.1 General

Each business continuity plan should identify its purpose, scope and objectives in a form that is clear to the teams that use it. Links to other required or relevant documented procedures or documents should be clearly stated and the method of obtaining and accessing them described. The business continuity plan should also include:

— activation criteria and procedures;

— implementation procedures;

— communication requirements and procedures;

— internal and external interdependencies and interactions;

— resource requirements;

— reporting requirements;

— information flow and documentation processes.

8.4.4.3.2 Guidance and supporting information

Each plan should include:

a) roles, responsibilities and authorities:

   1) defined roles, responsibilities and authorities for people and teams who will use the plan;

   2) guidelines and criteria regarding who has the authority to invoke the plan and under what circumstances (this may include defined escalation stages);

b) activation criteria:

   1) a process for activating the organization's response to a disruption and, within each documented procedure, its activation criteria and procedures (it can be relevant to consider whether this is within or outside normal working hours);

   2) meeting locations with suitable alternatives;

c) operation parameters:

   1) identification of actions and tasks to be performed, particularly in relation to how the organization will continue or will recover its prioritized activities within predetermined time frames;

   2) relevant resource requirements (see 8.3.4);

   3) the means for recording information about the incident, actions taken and decisions made;

d) supporting information for coordination and communication:

   1) contact details for team members and others with roles and responsibilities; the organization should be aware of applicable legal requirements in relation to the protection of information and should retain evidence of compliance;

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

e) standing-down criteria:

1) mechanisms for standing down once the incident has passed;

2) instructions to be followed.

8.4.4.3.3 Usability

As with any form of documented information (see 7.5.3), the organization should ensure that business continuity plans are usable and available whenever and wherever they are needed. To ensure that the operation of business continuity plans is not adversely affected by the disruption, the organization may need to take precautions (e.g. separating teams and recovered ICT systems across multiple locations). Total separation for all scales and types of disruption is not always achievable and it may be necessary to identify limitations and agree them with top management. Limitations can be expressed in terms of distance, minimum personnel or severity and may be influenced by the response of public agencies to severe or widespread disruptions.

8.4.4.4 Incident/strategic management

The aim of incident management is to ensure that the organization's response to a disruption 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, and should address all facilities that the team managing the incident and other response teams could need.

8.4.4.5 Communications

Communications procedures may be included in incident management or other team's response procedures. If there are multiple teams, they should work in close cooperation.

Communications that will be delivered and received during the incident should be managed and coordinated. Procedures should contain:

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

b) details on the organization's media response following an incident, which may include:

1) the incident communications strategy;

2) preferred interface with the media;

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

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

It is important that the timing and content of internal and external communications is consistent. To build confidence, trust and motivation, internal communication is a priority.

Pre-prepared information can be especially useful in the early stages of an incident. It will enable the team to provide details about the organization and its business activities while details of the incident are still being established.

It may be appropriate to:

— establish a suitable venue for liaising with the media or other groups of interested parties;

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

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

— 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.

8.4.4.6 Safety and welfare

Organizations have a duty of care to 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 physical and learning disabilities or other specific needs (e.g. pregnancy, temporary disability due to injury). Planning in advance to meet these requirements can reduce risk and reassure those affected. The long-term impacts of incidents cannot be underestimated. The organization should develop appropriate solutions, including consideration of relevant social and cultural issues, to promote physical and psychological recovery within the organization.

The following elements of welfare response should be included:

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

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

— 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 helplines;

— physical rehabilitation and psychological support.

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.

8.4.4.7 Salvage and security

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

— salvage priorities for facilities, equipment (including ICT systems) and documented information (taking into consideration information security and privacy requirements);

— 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 can limit impacts and enable a more rapid return to business as usual.

8.4.4.8 Resumption of prioritized activities

There should be procedures that specify:

— the prioritized activities to be resumed;

— the timescales within which they are to be resumed;

— capacities at which prioritized activities are to be resumed;

— the situations in which the procedure may be utilized.

Each procedure 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;

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

8.4.4.9 ICT systems

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

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

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

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

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

— the timetable of availability and capacity requirements allowing activities to meet their RTOs.

ISO/IEC 27031 provides further guidance.

8.4.5 Recovery

The organization should pre-determine how it will return to business as usual following a disruption and should have documented procedures to restore and return business operations from the temporary measures adopted during an incident. These should address relevant audit and corporate governance requirements.

The purpose of recovery is to re-establish business activities to support normal working following a disruption. Returning to business as usual may be achieved by:

— repairing the damage resulting from the incident;

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

— moving to a new location.

How best to return to business as usual will depend on the severity of the damage caused by the incident and estimates of how long it could take to establish the necessary facilities.

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

— establish recovery resources and infrastructure;

— operate at recovery facilities;

— restore damaged facilities;

— secure emergency procurement and funding;

— salvage equipment in damaged facilities;

— make claims against existing insurance policies;

— obtain additional people to support the recovery effort;

— select options for restoring and returning to business as usual;

— migrate operations to recovery facilities;

— recover lost documented information;

— communicate with relevant interested parties at appropriate frequencies;

— normalize operations at the restored facilities;

— conduct a post-recovery review;

— 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 that need to be met (see 8.3.4).

8.5 Exercise programme

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 develops teamwork, competency, confidence and knowledge, and should include those who could be required to use the procedures.

8.5.2 Design of the exercise programme

Robust and realistic exercises identify areas for improvement even in well-designed procedures. The organization should design an exercise programme that validates over time the effectiveness of its business continuity strategies and solutions, plans and procedures.

Establishing an exercise programme allows for a coordinated approach to building, evolving and maturing the organization's capabilities. The programme should cover individual plans, people (including those from external organizations), capabilities and resources that contribute to the organization's strategic objectives.

Top management should ensure that exercise programme objectives are set and a competent person is assigned to manage the exercise programme. The scope of an exercise programme should be based on the size and nature of the organization undertaking exercising, and the scope, functionality, complexity and the level of maturity of the plans and capabilities being exercised. 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.

The exercise programme should be flexible, considering 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 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.

To ensure that exercises are conducted effectively and efficiently within specified time frames, the exercise programme should include the following:

— needs analysis;

— endorsement by top management;

— clear objectives;

— the extent, number, types, duration, locations and schedules of exercises;

— appropriate personnel to support the programme;

— necessary resources and budget;

— processes for handling confidentiality, information security, health and safety, and other similar matters.

The exercise programme should provide assurance over time that the organization's overall response will be effective. The programme, when implemented, should:

— exercise the technical, logistical, administrative, procedural and other operational aspects of the procedures;

— exercise all persons with responsibilities within the procedures, including those from external organizations;

— exercise the business continuity arrangements and infrastructure (including, for example, command centres and work areas);

— validate the technology and telecommunications recovery, including the availability and relocation of staff;

— exercise response teams in the management of impacts arising from disruption of the supply chain.

The organization should monitor and measure the implementation of the exercise programme to ensure that its objectives are achieved. The exercise programme should be reviewed to identify improvements.

8.5.3 Exercising business continuity plans

Exercises, including tests, 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);

— 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 activities being disrupted 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 information obtained from previous disruptions.

The effectiveness of some aspects of business continuity will require that particular individuals or those occupying specific positions have particular knowledge, skills and understanding. 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:

— verification that activity RTOs (see 8.2.2) and RTOs for the dependencies and supporting resources of prioritized activities (see 8.3.2.3) are achievable;

— confidence that information and data required by activities are appropriately current (see 8.3.4.3);

— improved understanding of dependencies on the business continuity of suppliers and other interested parties;

— improved awareness of the organizational context and priorities;

— improved understanding of the content and use of business continuity procedures;

— improved confidence in responding to incidents;

— an opportunity to improve capabilities;

— an assessment of the utility and applicability of business continuity solutions;

— an evaluation of the adequacy of developed capabilities and resource allocations;

— an identification of previously undocumented requirements and practices employed in managing disruptions;

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

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

— improved confidence of interested parties regarding the organization's preparedness;

— 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 a number of factors, including:

— the context of the organization;

— the objectives for the exercise;

— the maturity of the exercise programme;

— the participants' experience;

— budget;

— participant availability;

— the tolerance of the organization to operational disruption caused by holding the exercise.

The organization should act on the results of its exercising to implement approved changes and improvements.

Many different names are given to the different types of exercises that can be carried out, but they generally fall into the following categories.

— Discussion: Discussion-based exercises are designed to familiarize participants with business continuity plans and procedures in a low stress environment.

— Simulation: Operations-based exercises are designed to be more realistic and challenging. They can be carried out in the normal operational environment, alternative premises or command centres.

Examples are provided in Table 6.

Table 6 — Sample descriptions of exercise methods

Category	Method	Description
Discussion	Plan review	Plan reviews are informal reviews of plans and procedures that are used to familiarize participants with new or updated content. They are useful as a starting point when plans and procedures are first developed or when they are revised significantly. A plan review can typically be conducted in 1 h to 2 h.
	Table-top (on-site)	On-site table-top exercises use simple scenarios to familiarize participants with plans and procedures in a low-stress environment. They can also be used to review business continuity strategies and solutions for validation and improvement. An on-site table-top exercise is usually the first type of formal exercise conducted by an organization and can typically be conducted in in 2 h to 3 h.
	Table-top (off-site)	Off-site table-top exercises are usually conducted at alternative premises or at a command centre with the purpose of reviewing business continuity plans and procedures. The exercise typically uses a simple scenario. The key difference from an on-site table-top is that the review takes place away from the normal operational environment. An off-site table-top exercise can typically be conducted in 2 h to 3 h excluding transportation time.
Simulation	Workshop (single or multiple plans)	Plan-based workshops are usually conducted off-site at alternative premises using reasonably complex scenarios. Exercise participants may represent a single plan or multiple plans depending upon the scope of the exercise. The purpose is for teams to practise working together and making decisions under more stressful time frames. A workshop exercise covering multiple plans can typically be conducted in 3 h to 5 h depending on the complexity of the plans and the scenario.
	Workshop (single or multiple locations)	Location-based workshops are usually conducted off-site at alternative premises using scenarios that impact one or more locations. The purpose of the exercise is for teams from different locations to practise working together and making joint decisions. A workshop exercise covering multiple locations can typically be conducted in 3 to 5 h depending on the number of locations involved and the complexity of the scenario.
	Workshop for the entire organization (full scale)	Full-scale exercises are designed to prepare participants for disruptions that impact the entire organization and require activation of the business continuity plan. They are complex, high-stress exercises that are carefully planned and controlled to ensure that they achieve their objectives and do not cause a disruption. A full-scale exercise can take any time between half a day and a week depending on its complexity and the number of people involved.

As part of the exercise, a review should be scheduled with all participants to discuss the 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.

The benefits of exercising and testing include:

— validation of assumptions, business continuity solutions and the scopes of business continuity plans;

— 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;

— development of participants' competency and awareness.

ISO 22398 provides further guidance on the types of exercise as well as guidance on planning, conducting and improving exercise programmes.

8.6 Evaluation of business continuity documentation and capabilities

8.6.1 General

The organization should conduct evaluations of its business impact analysis, risk assessment, strategies and solutions, business continuity plans and procedures in order to ensure their continuing suitability, adequacy and effectiveness.

The evaluations should address the possible need for changes to the policy, objectives and other elements of the BCMS based on, for example, the exercise results, post-incident reviews and changing organizational circumstances.

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

Evaluations should verify that:

— all products and services and their supporting activities and resources have been identified and included in the organization's business continuity solutions;

— the organization's business continuity policy, solutions and business continuity procedures accurately reflect its priorities and business requirements;

— 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 disruption;

— the organization's business continuity solutions are effective, up-to-date and fit-for-purpose;

— the organization's exercising and maintenance programmes have been effectively implemented;

— business continuity solutions and procedures incorporate improvements identified during incidents and exercises and in the maintenance programme;

— the organization has an ongoing programme for business continuity training and awareness;

— business continuity procedures have been effectively communicated to relevant staff, and that these staff understand their roles and responsibilities;

— the business continuity arrangements that suppliers and partners have in place for dependencies of prioritized activities are appropriate and adequate;

— the organization is sufficiently compliant with applicable legal and regulatory requirements, and industry best practices, and is in conformity with business continuity policy and objectives;

— change control processes are in place and operate effectively.

8.6.2 Measuring effectiveness

Measuring the effectiveness of business continuity plans, procedures and capabilities should include the business continuity arrangements for outsourced activities and the business continuity of suppliers and partners that prioritized activities depend on.

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

— backup data are sufficiently current to resume activities and resources within specified RTOs;

— 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 RTO have been demonstrated;

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

When the organization experiences a disruption, a review should be undertaken. This may include:

— identifying the nature and cause of the disruption;

— assessing the adequacy of management's response;

— assessing the organization's effectiveness in meeting its RTOs;

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

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

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

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

8.6.3 Outcomes

Outcomes indicative of effective business continuity plans, procedures and capabilities may include the following:

— an incident management capability is enabled and provides an effective response;

— 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;

— regular exercising ensures that staff are trained to respond effectively to a disruption;

— the requirements of interested parties are understood and able to be delivered;

— staff receive adequate support and communications during a disruption;

— the organization's reputation is protected;

— a demonstration of legal and regulatory compliance;

— financial controls are maintained throughout an incident;

— the organization can demonstrate an enhanced level of resilience to its customers and other interested parties.

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

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.1.1 General

Procedures for monitoring, measuring, analysing and evaluating the performance and the effectiveness of the BCMS should include:

a) determining the methods for monitoring, measurement analysis and evaluation, including:

   1) specifying what is to be monitored and measured;

   2) identifying how, when and by whom the monitoring and measuring should be performed;

   3) setting performance metrics, including qualitative and quantitative measurements that are appropriate to the organization and ensure valid results;

   4) recording data and results to facilitate subsequent corrective action analysis;

b) examining historical evidence;

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

d) measuring compliance of the BCMS with applicable statutory and regulatory requirements;

e) monitoring nonconformity and other evidence of deficient BCMS performance.

9.1.2 Retention of evidence

The organization should retain appropriate documented information of all periodic evaluations and their results.

9.1.3 Performance evaluation

The organization should use performance indicators to evaluate the performance and effectiveness of the BCMS and its outcomes in order to identify successes and areas requiring correction or improvement. The data obtained can be used to identify patterns and to enable the organization to obtain information regarding the performance of the BCMS.

9.2 Internal audit

9.2.1 General

The organization should conduct internal audits at planned intervals to assess the performance of the BCMS.

Internal audits of the BCMS provide a mechanism for measuring the extent to which the BCMS is achieving its objectives, conforms to its planned arrangements, and has been properly implemented and maintained, and for identifying opportunities for improvement. Internal audits of the BCMS should be conducted at planned intervals to determine and provide information to top management on the appropriateness and effectiveness of the BCMS as well as to provide a basis for setting objectives for continual improvement of BCMS performance.

9.2.2 Audit programme(s)

The organization should establish an audit programme (see ISO 19011) to direct the planning and conduct of audits, and to 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.

Internal audit programmes should be based on the full scope of the BCMS, however, each audit need not cover the entire system all at once. Audits may be divided into smaller parts, so long as the audit programme ensures that all organizational units, functions, activities, 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 to 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 able to do so impartially and objectively. In smaller organizations, auditor independence may be demonstrated by an auditor being free from the responsibility for the activity being audited.

9.3 Management review

9.3.1 General

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.

9.3.2 Management review input

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 supply chain and effectiveness of supply chain continuity arrangements;

— other changes to the organization and its context (see 4.1) and feedback from interested parties (see 4.2) that could impact the management system;

— 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 and any exclusions (see 4.3), 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 ongoing 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 can require a review of the BCMS.

c) Incident experience: A review should be performed following a response to a disruption, even if the response procedure was not activated. If activated, the review should consider the history of the response procedure, how it worked and why it was activated. If the response procedure was not activated, the review should examine why it wasn't and whether this was the correct decision. It may also be beneficial to review disruptions affecting other organizations in the same sector and similar industries.

9.3.3 Management review outputs

9.3.3.1 Improvement of the BCMS

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

— variations to the scope;

— updates to business continuity strategies and solutions;

— changes to controls and how their effectiveness is measured.

9.3.3.2 Retention of documented information

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;

— take appropriate action relating to these results.

10 Improvement

10.1 Nonconformity and corrective action

10.1.1 General

The organization should determine opportunities for improving the BCMS and implement the actions necessary to achieve its intended outcomes.

10.1.2 Occurrence of nonconformity

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 the identification of:

— the non-fulfilment of a requirement;

— an ineffective planning approach;

— weaknesses associated with the BCMS.

Once identified, these should be acted upon in a timely manner to prevent further occurrence of the situation, as well as to identify and address root causes. The procedures should enable ongoing detection, analysis and elimination of actual and potential causes of nonconformities.

Nonconformities should be identified and dealt with in a timely manner, as should the corrective actions that address them. The corrective actions 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.

The organization should improve the performance and effectiveness of the BCMS even when there is no evidence of nonconformity. Improvements can include correction, corrective action, innovation and re-organization

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

10.1.3 Retention of documented information

The organization should retain documented information as evidence of the:

— nature of the nonconformities and subsequent actions, if any, taken;

— results of corrective actions, if any, taken.

10.2 Continual improvement

Continual improvement, in terms of the suitability, adequacy and effectiveness of the BCMS, operates at all levels within the PDCA cycle and should be driven by the business continuity policy and objectives, audit results, analysis of disruptions, management review, ambitions and the desired maturity level.

Continual improvement requires a process that identifies opportunities and a process to manage them. The continual improvement process should follow the same basic process as used for corrective actions and should include the following:

— identify what to address and the present condition (room for improvement);

— identify the present process and controls;

— determine what changes to implement (improvement).

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.

The organization can achieve improvement through the effective application of BCMS processes, such as leadership (see Clause 5), planning (see Clause 6) and performance evaluation (see Clause 9). Top management should also consider opportunities for improvement in the BCMS, which can come from changes in:

— the context of the organization (e.g. failure of a competitor);

— the internal structure of the organization (e.g. acquisition of additional locations or staff);

— the means of production or delivery (e.g. technological change, infrastructure improvements);

— evolving methodologies or the availability of new recovery methods (e.g. new standby facilities or network technology);

— technology and practices, including new tools and techniques.

These should be evaluated to establish their potential benefit to the organization.

Bibliography

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

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

[3] ISO/TS 22317, *Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)*

[4] ISO/TS 22318, *Societal security — Business continuity management systems — Guidelines for supply chain continuity*

[5] ISO/TS 22330, *Security and resilience — Business continuity management systems — Guidelines for people aspects of business continuity*

[6] ISO/TS 22331, *Security and resilience — Business continuity management systems — Guidelines for business continuity strategy*

[7] ISO 22398, *Societal security — Guidelines for exercises*

[8] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

[9] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[10] ISO 31000, *Risk management — Guidelines*

ISO 22313:2020(E)

ICS 03.100.70; 03.100.01

Price based on 55 pages