DRAFT INTERNATIONAL STANDARD ISO/DIS 22313

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

Voting begins on **2011-12-13** Voting terminates on **2012-05-13**

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

Societal security — Business continuity management systems — Guidance

Sécurité sociétale — Gestion de la continuité des affaires — Lignes directrices

ICS 03.100.01

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

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

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

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

Contents

Page

Foreword

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

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

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

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

Introduction

0 Introduction

0.1 General

This International Standard provides guidance to ISO 22301 for setting up and managing an effective business continuity management system (BCMS)

A BCMS emphasizes the importance of:

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

— implementing and operating controls and measures for managing an organization's overall business continuity risks;

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

— continual improvement based on objective measurement.

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

a) a policy;

b) people with defined responsibilities;

c) management processes relating to:

   1) policy;

   2) planning;

   3) implementation and operation;

   4) performance assessment;

   5) management review;

   6) improvement.

d) a set of documentation providing auditable evidence; and

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

Business continuity contributes to a more resilient society. The wider community and the organization's environment impact on the organization and therefore other organizations may need to be involved in the recovery process.

0.2 The Plan-Do-Check-Act cycle

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

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

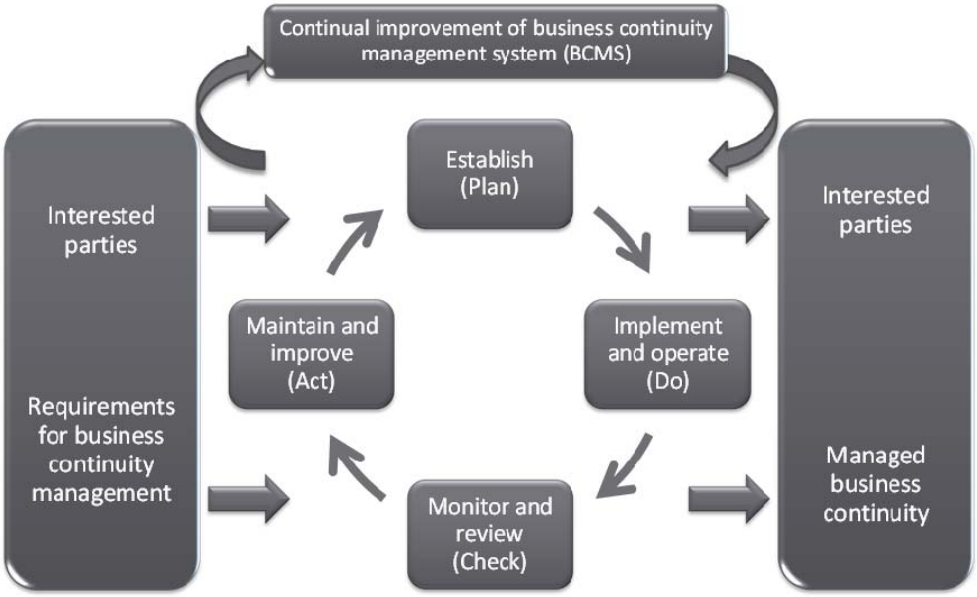

Figure 1 —PDCA cycle applied to BCMS processes

Table 1 – Explanation of PDCA cycle

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

0.3 Business continuity management

Business continuity management (BCM) is about preparing an organization to deal with disruptive incidents that might otherwise prevent it from achieving its objectives.

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

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

BCM is not complicated. It involves:

a) Identifying the organization's key products and services;

b) Identifying the prioritized activities and resources required to deliver them;

c) Evaluating the threats to these activities and their dependencies;

d) Putting arrangements in place to resume these activities following an incident; and

e) Making sure that these arrangements will be effective in all circumstances.

BCM may be effective in dealing with both sudden incidents, for example, caused by explosions, and gradual incidents, for example, flu pandemics.

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

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

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

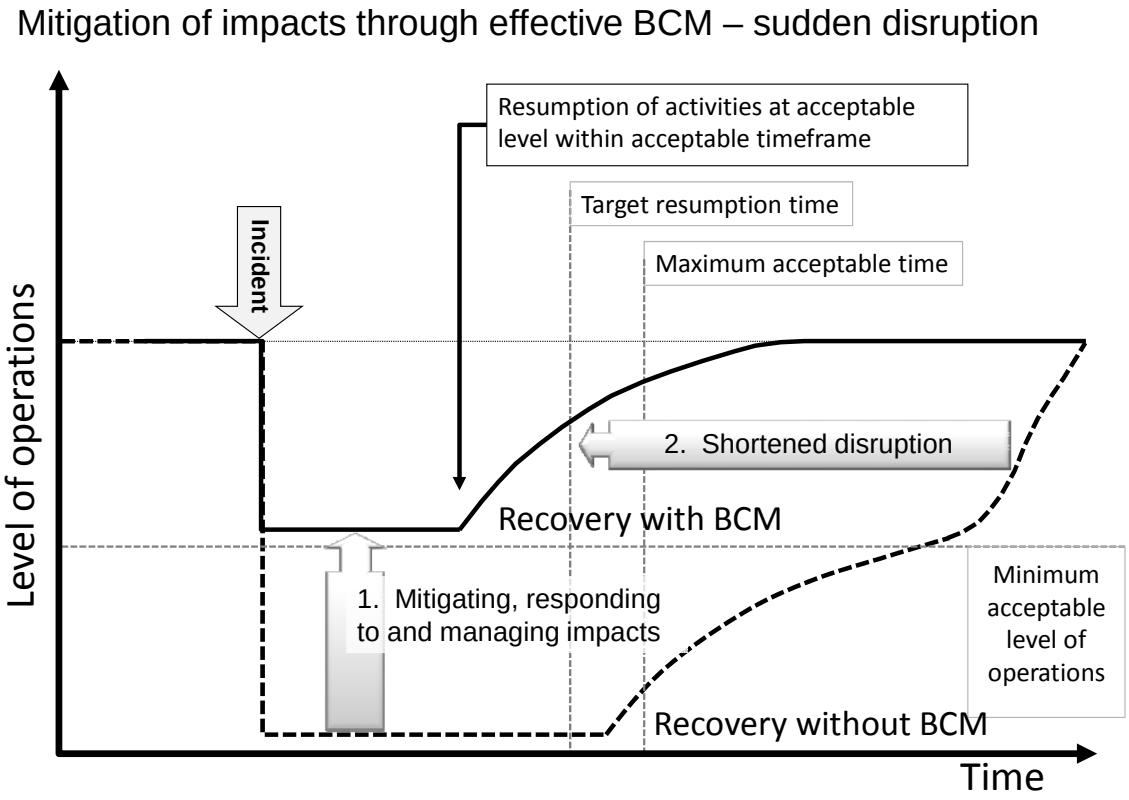

Figure 2 — Illustration of BCM being effective for sudden disruption

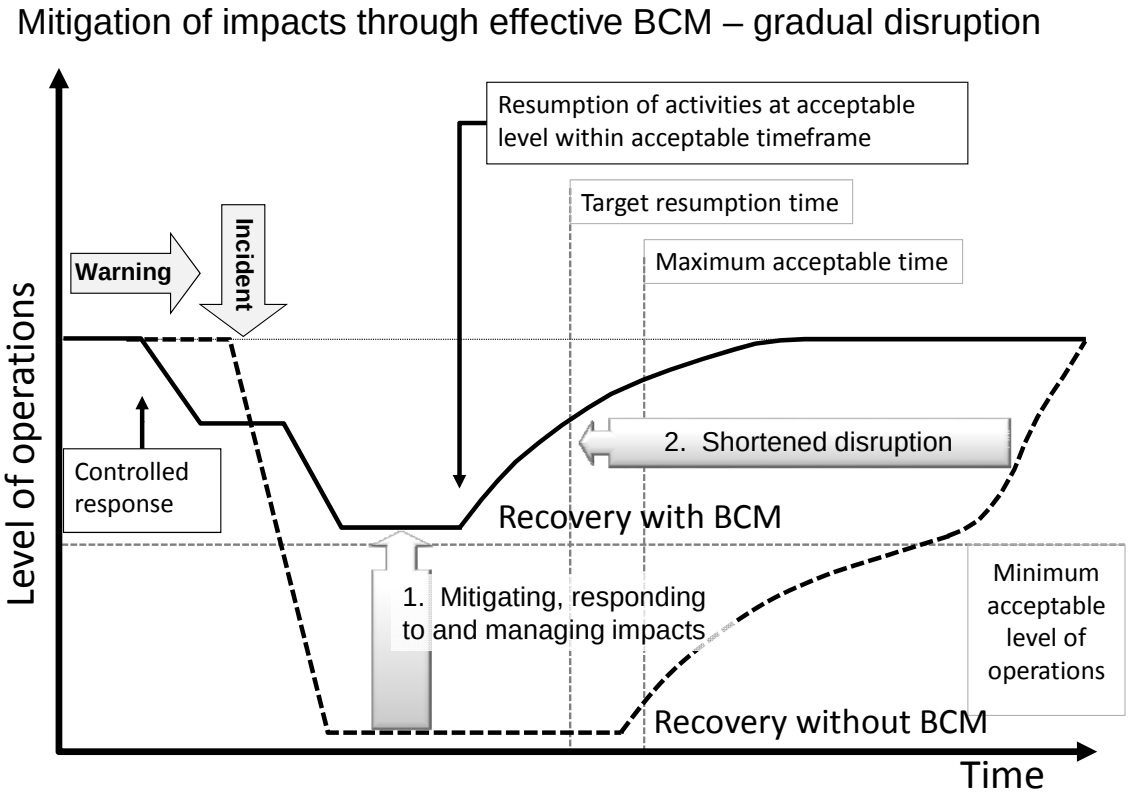

Figure 3 — Illustration of BCM being effective for gradual disruption (e.g. approaching pandemic)

Societal security — Business continuity management systems — Guidance

1 Scope

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

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

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

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

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

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

This International Standard should not be used to assess an organization's ability to meet its own business continuity needs, nor any customer, legal or regulatory needs. Organizations wishing to do so should use the ISO 22301, Societal security — Business continuity management systems — Requirements, to demonstrate conformance to others or seek certification/registration of its BCMS by an accredited third party certification body.

2 Normative references

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

ISO 22300, *Societal security — Terminology*

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

ISO Guide 73, *Risk management —Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC Guide 73:2009, ISO 22300 and the following apply.

NOTE It should be noted that the terms and definitions are harmonized between ISO 22301 and ISO 22313.

3.1
activity
process or set of processes undertaken by an organization (or on its behalf) that produces or supports one or more products and services

NOTE Examples of such processes includes accounts, call centre, IT, manufacture, distribution.

3.2
audit
systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

NOTE 1 An audit may be an internal audit (first party) or an external audit (second party or third party), and it may be a combined audit (combining two or more disciplines).

NOTE 2 Audit evidence" and "audit criteria" are defined in ISO 19011.

3.3
business continuity
strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level

3.4
business continuity management
holistic management process that identifies potential threats to an organization and the impacts to business operations of those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities

3.5
business continuity management system
BCMS
that part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity

NOTE The management system includes organizational structure, policies, planning activities, responsibilities, procedures, processes and resources.

3.6
business continuity plan
documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption

NOTE Typically this covers resources, services and activities required to ensure the continuity of critical business functions.

3.7
business continuity programme
ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management

3.8
business impact analysis
process of analyzing operational functions and the effect that a disruption might have upon them

3.9
competence
ability to apply knowledge and skills to achieve intended results

3.10
conformity
fulfillment of a requirement

[SOURCE: ISO 22300]

continual improvement
recurring activity to enhance performance

[SOURCE: ISO 22300]

3.11
correction
action to eliminate a detected nonconformity

[SOURCE: ISO 22300]

3.12
corrective action
action to eliminate the cause of a nonconformity and to prevent recurrence

[SOURCE: ISO 22300]

3.13
document
information and its supporting medium

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

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

3.14
effectiveness
extent to which planned activities are realized and planned results achieved

[SOURCE: ISO 22300]

3.15
event
occurrence or change of a particular set of circumstances

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

NOTE 2 An event may consist of something not happening.

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

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

[SOURCE: ISO/IEC GUIDE 73]

3.16
exercise
instrument to train for, assess, practice, and improve performance and capabilities in a controlled environment

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

3.17
incident
event that might be, or could lead to, a business disruption, loss, emergency or crisis

3.18
infrastructure
system of facilities, equipment and services needed for the operation of an organization

3.19
interested party
person or group of people that holds a view that may affect the organization

3.20
internal audit
audit conducted by, or on behalf of, the organization itself for management review and other internal purposes, and which might form the basis for an organization's self-declaration of conformity

NOTE In many cases, particularly in smaller organizations, independence may be demonstrated by the freedom from responsibility for the activity being audited.

3.21
invocation
act of declaring that an organization's business continuity arrangements need to be put into effect in order to continue delivery of key products or services

3.22
management system
set of interrelated or interacting elements of an organization to establish policies and objectives, and processes to achieve those objectives

NOTE 1 A management system may address a single discipline or several disciplines.

NOTE 2 The system elements include the organization's structure, roles and responsibilities, planning, operation, etc.

NOTE 3 The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

[SOURCE: ISO 22300]

3.23
maximum acceptable outage
MAO
time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable

NOTE See also maximum tolerable period of disruption in 3.25.

3.24
maximum tolerable period of disruption
MTPD
time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable

NOTE See also maximum acceptable outage in 3.24.

3.25
minimum business continuity objective
MBCO
minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption

3.26
monitoring
determining the status of a system, a process or an activity

NOTE To determine the status there may be a need to check, supervise or critically observe.

[SOURCE: ISO 22300]

3.27
mutual aid agreement
pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement

3.28
nonconformity
non-fulfillment of a requirement

[SOURCE: ISO 22300]

3.29
objective
result to be achieved

NOTE 1 An objective may be strategic, tactical or operational.

NOTE 2 An objective may be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a business continuity objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

[SOURCE: ISO 22300]

3.30
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

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

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

[SOURCE: ISO 22300]

3.31
outsource (verb)
make an arrangement where an external organization performs part of an organization's function or process

NOTE An external organization is outside the scope of the management system, although the outsourced function or process is within the scope.

3.32
performance
measurable result

NOTE 1 Performance may relate either to quantitative or qualitative findings.

NOTE 2 Performance may relate to the management of activities, processes, products (including services), systems or organizations.

3.33
performance evaluation
process of determining measurable results

3.34
personnel
people working for and under the control of the organization

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

3.35
policy
intentions and direction of an organization as formally expressed by top management

[SOURCE: ISO 22300]

3.36
procedure
specified way to carry out an activity or a process

3.37
process
set of interrelated or interacting activities which transforms inputs into outputs

3.38
products and services
beneficial outcomes provided by an organization to its customers, recipients and interested parties

EXAMPLE Manufactured items, car insurance and community nursing

3.39
prioritized activities
activities to which urgent priority must be given following an incident in order to mitigate impacts

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

[SOURCE: ISO 22300]

3.40
record
statement of results achieved or evidence of activities performed

3.41
recovery point objective
RPO
point to which information used by an activity must be restored to enable the activity to operate on resumption

NOTE May also be referred to as ‘maximum data loss’

3.42
recovery time objective
RTO
period of time following an incident within which product or service must be resumed, activity must be resumed, or resources must be recovered

NOTE For products, services and activities, the recovery time objective must be less than the time it would take for the adverse impacts that would arise as a result of not providing a product/service or performing an activity to become unacceptable.

3.43
requirement
obligatory need or expectation that is stated or implied

3.44
resources
all assets, people, skills, information, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that an organization has to have available to use, when needed, in order to operate and meet its objective

3.45
risk
effect of uncertainty on objectives

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

NOTE 2 Objectives may relate to different disciplines (such as financial, health and safety, and environmental goals) and may apply at different levels (such as strategic, organization-wide, project, product and process). An objective may be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a business continuity objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

NOTE 3 Risk is often characterized by reference to potential events (Guide 73, 3.5.1.3) and consequences (Guide 73, 3.6.1.3), or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (Guide 73, 3.6.1.1) of occurrence.

NOTE 5 Uncertainty is the state, even partial, of efficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

NOTE 6 In the context of business continuity management system standards, business continuity objectives are set by the organization, consistent with the business continuity policy, to achieve specific results. When applying the term risk and components of risk management, this should be related to the objectives of the organization that include, but are not limited to the business continuity objectives as specified in 6.2 of the text.

[SOURCE: ISO Guide 73]

3.46
risk appetite
amount and type of risk that an organization is willing to pursue or retain

3.47
risk assessment
overall process of risk identification, risk analysis and risk evaluation

[SOURCE: ISO Guide 73]

3.48
risk management
coordinated activities to direct and control an organization with regard to risk

[SOURCE: ISO Guide 73]

3.49
testing
procedure for evaluation; a means of determining the presence, quality, or veracity of something

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

NOTE 2 Testing is often applied to supporting plans.

3.50
top management
person or group of people who directs and controls an organization at the highest level

NOTE 1 Top management has the power to delegate authority and provide resources within the organization.

NOTE 2 An organization may for this purpose be identified by reference to the scope of the implementation of a management system.

[SOURCE: ISO 22300]

3.51
verification
confirmation, through the provision of evidence, that specified requirements have been fulfilled

3.52
work environment
set of conditions under which work is performed

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

[SOURCE: ISO 22300]

4 Context of the organization

4.1 Understanding of the organization and its context

The organization should determine external and internal factors that are relevant to establishing, implementing and maintaining the organization’s BCMS, and assigning priorities.

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

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

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

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

— supply chain commitments and relationships;

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

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

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

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

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

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

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

— interested parties within the organization;

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

— future opportunities and business priorities;

— perceptions, values and culture;

— standards and reference models adopted by the organization; and

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

4.2 Understanding the needs and expectations of interested parties

4.2.1 General

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

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

NOTE When establishing the BCM, the organization needs to be aware of not only 'those groups without whose support the organization would cease to exist', the Stanford Research Institute's definition of stakeholders, but additionally those who have an interest in the organization, such as the media, the public nearby, competitors and so on. Furthermore a stakeholder may have defined requirements that must be taken into account, whereas an interested party in most situations is not able to specify requirements or impose obligations.

When planning and implementing the BCMS, it is important to identify actions that are appropriate in relation to interested parties but differentiate between the different categories. For example, it is likely to be appropriate to communicate with all interested parties following a disruptive incident but it may not be appropriate to communicate with all interested parties during all stages of the business continuity programme referred to in 8.1.1.

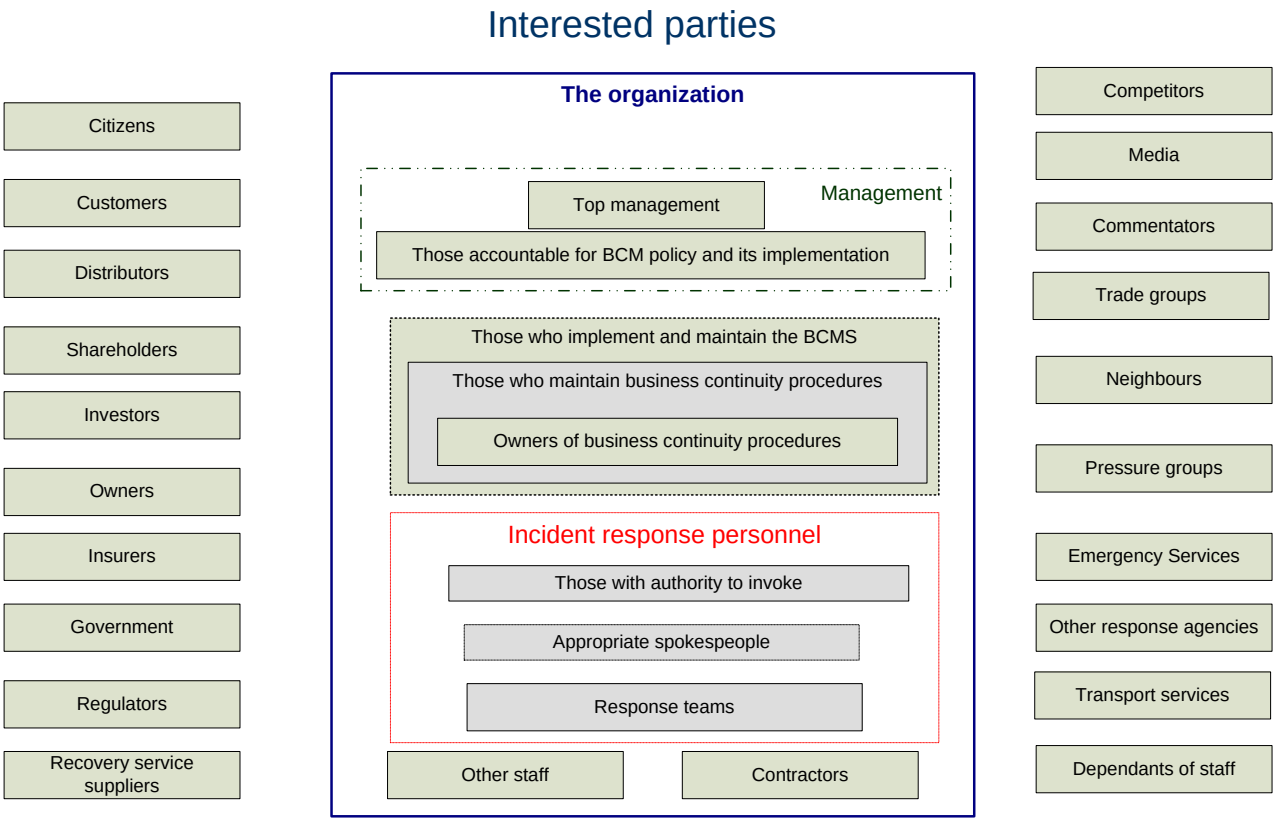

Figure 4 — Examples of interested parties to be considered in public and private sectors

4.2.2 Legal and regulatory requirements

All management systems should operate within the framework of the legal and regulatory environment in which the organization operates. The organization should therefore establish procedures that will enable it to identify and accommodate in its BCMS all applicable legal and regulatory requirements that relate to the continuity of its operations and interested parties. The information regarding these requirements should be documented, kept up-to-date and communicated to affected employees and other interested parties.

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

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

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

a) Incident Response: including emergency management and health, safety and welfare legislation;

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

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

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

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

4.3 Determining the scope of the management system

4.3.1 General

The organization should determine the scope of the BCMS and ensure that it may be suitably communicated to interested parties. The boundaries and applicability of the BCMS should be clearly apparent and the scope should take into account the issues identified in Clause 4.1 (Understanding of the organization and its context) and Clause 4.2 (Understanding the needs and expectations of interested parties).

The scope defines which part of the organization's products and services, activities and/or processes, locations, functions, etc. the BCMS applies to.

The organization should clearly document the scope and context of the BCMS and management's commitment to it.

4.3.2 Scope of the BCMS

The scope of the BCMS should be defined in terms appropriate to the size, nature and complexity of the organization.

The wording of the scope should:

a) ensure that the organization's products and services, activities, resources, partnerships, supply chains, and interested parties relationships included within the scope are clearly distinguishable;

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

c) identify how the BCMS fits into the organization's overall risk management strategy.

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

The organization should, in an appropriate manner to its size, nature and complexity, define and document the scope of its BCMS in terms of:

— its requirements for business continuity taking into consideration its mission, goals, legal responsibilities and internal and external obligations; and

— its operational objectives, products and services, activities and resources;

The purpose of this is to ensure coverage of all activities, locations, suppliers and outsourcing partners that have an impact on those products and services. The scope should identify the key products and services that support the organization's objectives, obligations and statutory duties. The purpose of this is to ensure coverage of all activities, locations, suppliers and outsourcing partners that have an impact on those products and services.

The scope should be consistent with the protection and preservation of the organization's integrity and its relationships with interested parties (e.g. key suppliers, outsourcing partners, the organization's supply chain vendors, customers and the community in which it operates).

Any exclusion from scope should be clearly documented, making sure that such exclusions do not undermine the performance and effectiveness of the BCMS, including its continuity capabilities.

4.4 Business continuity management system

The organization should establish an effective BCMS that conforms to the recommendations of this standard.

This implies the need to consider not only the individual requirements but also the processes that will need to be established and the way that they will interact.

5 Leadership

5.1 General

Management at all levels should clearly demonstrate support for the BCMS.

All levels of management should demonstrate leadership in their capacity to fulfill business continuity policy and objectives in support of top management. Demonstration may be achieved using techniques of motivation, engagement and empowerment.

5.2 Management commitment

Top management should demonstrate its commitment to the BCMS.

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

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

b) establishing business continuity policy and objectives in line with the purpose of the organization (refer 5.3);

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

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

e) ensuring the availability of sufficient resources (refer 7.1);

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

g) ensuring that internal BCMS audits are conducted (refer 9.2);

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

i) directing and supporting continual improvement (refer 10.2).

Management commitment may also be demonstrated by:

— operational involvement through steering groups;

— active participation in exercising and testing; and

— inclusion of BCM as a standing item at management meetings.

5.3 Policy

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

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

— provides a framework for objective setting;

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

— is communicated and understood within the organization and available to interested parties.

— is complementary to other relevant policies; and

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

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

The policy should also:

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

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

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

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

The business continuity policy may contain the following:

— Key terms;

— Funding commitment;

— References to other related policies;

— Management's intentions relating to service levels during the disruption;

— Set-up activities for establishing a business continuity capability; and

— On-going management and maintenance of the business continuity capability.

Set-up activities should include specification, end-to-end design, build, implementation and initial exercising of the business continuity capability.

On-going maintenance and management activities should include embedding business continuity within the organization, exercising business continuity procedures regularly, and updating and communicating them, particularly when there is significant change in premises, personnel, process, market, technology or organizational structure.

5.4 Organizational roles, responsibilities and authorities

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

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

The organization's top management should appoint (a) specific management representative(s) who, irrespective of other responsibilities, should have defined roles, responsibilities and authority for:

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

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

— promoting awareness of the programme throughout the organization; and

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

This person may:

— be known as the 'business continuity manager';

— may hold other responsibilities within the organization; and

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

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

The organization may appoint other bodies, such as a steering committee, to oversee the implementation of the business continuity programme.

All roles, responsibilities and authorities in the business continuity programme should be defined and documented and be subject to audit.

6 Planning

6.1 Actions to address risks and opportunities

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

This should involve evaluating the need for a plan of action and, if necessary:

— integrating and implementing these actions into the BCMS process; and

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

6.2 Business continuity objectives and plans to achieve them

Top management should ensure that appropriate objectives are established for agreed functions and levels within the organization, retain documented information relating to them and clearly state how they will be achieved.

These objectives should:

— be clearly stated;

— be consistent with the policy;

— be measurable;

— have time frames for their achievement;

— take account of applicable needs and requirements;

— enable opportunities to maintain or improve performance;

— be monitored and updated as appropriate.

In order to ensure that these objectives will be achieved, the organizations should determine:

— who will be responsible;

— what will be done and when it will be completed; and

— how the results will be evaluated.

Top management may set minimum business continuity objectives (MBCOs) for key products and services in order to establish the minimum acceptable levels required during a disruption to achieve the organization's business objectives

7 Support

7.1 Resources

7.1.1 General

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

Management should ensure the availability of the resources needed to implement and control the business continuity management system and to meet the organization's BCM objectives, including responding to incidents.

Through top management, the organization should provide appropriate resources, capabilities, structures and support mechanisms that will:

a) achieve its business continuity policy, objectives and targets;

b) meet the changing requirements of the organization;

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

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

These should be provided in a timely and efficient manner.

7.1.2 BCMS resources

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

a) People and people-related resources, including:

   1) The time necessary to perform BCMS roles and responsibilities;

   2) Training, education, awareness and exercising;

b) Facilities, including appropriate work locations and infrastructure;

c) Technology, including applications that support effective and efficient programme management;

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

e) Information, including consideration of:

   1) Policies;

   2) Interested parties (refer figure 4 on page X);

   3) Legal documents (e.g. contracts, insurance policies, title deeds, etc.); and

   4) Other services documents (e.g. contracts and service level agreements).

7.1.3 Incident response personnel

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

The incident response personnel should form a group that is responsible for managing any disruptive incident that significantly impacts or has the potential to significantly impact the organization. The responsibilities of this team may include and, where applicable, there should be procedures for:

a) Incident detection and escalation;

b) Incident assessment including confirmation of the nature and extent of the incident;

c) Triggering of an appropriate response;

d) Activation;

e) Evacuation;

f) Triage and first aid;

g) Parameter security;

h) Control of traffic;

i) Emergency operations centre establishment and operations;

j) Liaison with emergency services and local authorities;

k) Liaison with the organization’s crisis communication / public relations team;

l) Operations;

m) Coordination and communication of the incident response; and

n) Post incident analysis and reporting.

All personnel who are in this group should have clearly defined responsibilities and authorities that apply before, during and after the incident.

7.2 Competence

The organization should establish an appropriate and effective system for managing competence.

Management should determine the competences required for all BCMS roles and responsibilities and the awareness, knowledge, understanding and skills needed to fulfill them. All persons assigned roles within the organization should demonstrate the competencies required and be provided with training, education, development and other support needed to do so. This may be referred to as a competence development programme that may include:

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

— Identification of training, education, development and other support needed to attain competences;

— Provision of training and mentoring;

— Knowledge sharing;

— Job sharing;

— Hiring or contracting competent persons;

— Design and development of a personal development programme;

— Selection of suitable methods and materials;

— Verification of conformity with BCMS training requirements;

— Training of target groups;

— Documentation and monitoring of training received;

— Evaluation of training received against defined training needs and requirements; and

— Improvement of development programme as needed.

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

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

a) Planning and implementation of the BCMS:

    1) Business continuity programme management;

    2) Conducting a business impact analysis;

    3) Developing and implementing business continuity documentation;

    4) Running an exercise programme;

5) Risk assessment; and

6) Communications skills;

b) Incident response and business recovery:

1) Evacuation management;

2) Shelter-in-place;

3) Check-in processes to account for employees;

4) Arrangements at alternate worksites; and

5) Handling of media inquiries by the company.

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

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

Changes in the business environment and operations affect the approach and manner in which business continuity activities are planned, designed and implemented. The organization may demonstrate an ability to track and keep in tune with industry BCM trends by actively participating in industry BCM activities which may include:

— membership in industry BCM interest group; and

— attendance at local or global BCM conferences.

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

— organizing committee of conferences and seminars; and

— presentation of paper at conferences and seminars.

Competence may be reinforced by:

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

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

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

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

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

7.3 Awareness

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

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

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

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

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

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

— their role and responsibility in achieving conformity with the requirements of the BCMS and reporting of potential hazards or threats.

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

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

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

An organization with a positive business continuity culture will:

— develop a business continuity programme more efficiently;

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

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

— minimize the likelihood and impact of disruptions.

Development of a BC culture is supported by:

— involvement of all personnel in the organization;

— leadership from managers;

— assignment of responsibilities;

— performance indicators;

— awareness raising;

— skills training; and

— exercising business continuity procedures.

An awareness programme may include:

— a consultation process with staff throughout the organization concerning the implementation of the business continuity programme;

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

— inclusion of BCM on relevant web pages and intranets;

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

— selective publication of post event review reports following incidents;

— briefings for top management;

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

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

— establishing appropriate in-house processes.

7.4 Communication

The organization should have effective communication and consultation procedures for the exchange of information with interested parties.

These should include:

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

b) External communication with customers, partner entities, local community, and other interested parties, including the media;

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

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

e) Alerting interested parties potentially impacted by an actual or impending incident;

f) Ensuring availability of the means of communication during a disruptive incident;

g) Facilitating structured communication with appropriate authorities and ensuring the interoperability of multiple responding organizations and personnel, where appropriate; and

h) Operating and testing of communications capabilities intended for use during disruption of normal communications.

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

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

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

7.5 Documented information

7.5.1 General

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

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

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

The documentation recommended by this standard should include:

— Business continuity policy;

— BCMS and BCM objectives;

— Business impact analysis (BIA);

— Risk assessment;

— Business continuity options;

— Awareness programme;

— Training programme;

— Business continuity procedures;

— Business continuity plans;

— Exercise schedule and reports; and

— Service level agreements and contracts.

Documented information relating to the BCMS may include:

— Organization and individual training programmes;

— Evidence of process monitoring and performance;

— Evidence of inspection, maintenance and calibration;

— Pertinent contractor and supplier documentation including written contracts;

— Post event reports following incidents and near hits;

— Reports showing results, analysis and conclusions from exercises and tests;

— Audit results;

— Management review results;

— External communications decision;

— Applicable legal and regulatory documentation and evidence of compliance;

— Minutes showing discussions and conclusions relating to significant risk and impacts;

— Minutes and notes from management systems meetings; and

— Newsletters and other communications with interested parties.

Proper care should be taken to ensure the protection and non-disclosure of confidential information.

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

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

The organization's BCMS should comply with all documented information requirements for the BCMS as set out below.

7.5.2 Create and update

The organization should comply with all requirements for creating or updating documented information.

These should include:

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

— consideration of how the information will be captured and presented; and

— its review and approval for adequacy, when applicable.

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

The extent of documented information for the BCMS may differ from one organization to another due to:

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

— the complexity of activities and their interactions; and

— the competence of persons.

7.5.3 Control of documented information

All required documented information should be controlled.

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

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

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

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

a) distribute documented information;

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

c) approve documents for adequacy prior to issue;

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

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

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

g) ensure that documents remain legible and readily identifiable;

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

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

j) establish document retention and archival parameters; and

k) ensure the integrity of the documents by ensuring they are tamperproof, securely backed-up, accessible only to authorized personnel protected from damage, deterioration or loss and available when required for response or recovery.

8 Operation

8.1 Operational planning and control

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

A business continuity programme should be put in place in order to ensure that the organization's business continuity arrangements are managed appropriately and their effectiveness maintained.

Control mechanisms should include:

a) establishing criteria for relevant operational activities (these may relate to the supply of goods and services and may be contracted out or outsourced);

b) implementing controls, in accordance with the criteria; and

c) keeping documented information to demonstrate that these controls have been effective.

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

8.1.1 Elements of the business continuity programme

The business continuity programme comprises the following elements, as illustrated in the diagram below:

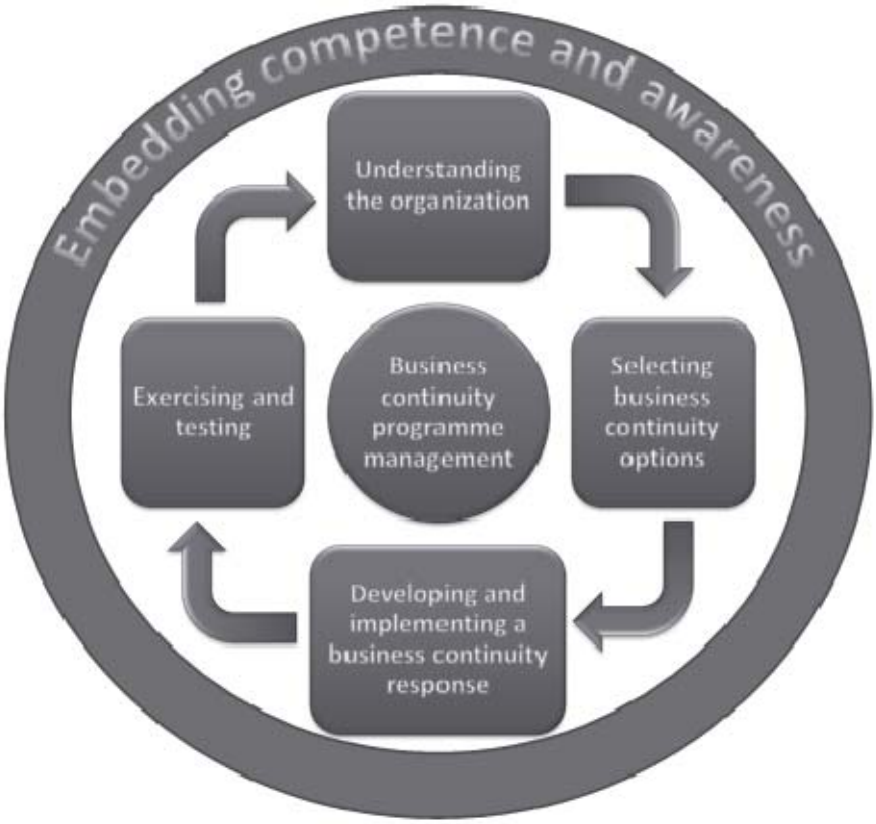

Figure 5 — Business continuity programme elements

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

a) **Business continuity programme management** (see Clauses 4 Context of the organization, 5 Leadership, 6 Planning, 7 Support, 8.1 Operational planning and control, 9 Performance evaluation, 10 Improvement)

Programme management is at the heart of the business continuity process. Effective programme management establishes and maintains the organization's approach to business continuity

b) **Embedding competence and awareness** (see Clauses 7.2 and 7.3)

Promoting awareness enables business continuity to become part of the organization's core values and ensures that the competence required for programme management and responding to an incident are maintained. It also instils the confidence of interested parties that the organization will cope effectively with disruptions.

c) **Understanding the organization** (see Clause 8.2 Business impact analysis and risk assessment)

Gaining agreement and understanding of priorities and requirements for business continuity is achieved through business impact analysis (BIA) and risk assessment (RA). The BIA enables the organization to prioritize for resumption, the activities that support its products and services. Risk assessment promotes understanding of the risks to these activities and their dependencies and the potential consequences if the risks were to materialize. This understanding enables to the organization to determine appropriate business continuity options

d) **Selecting business continuity options** (see Clause 8.3 Business continuity strategy)

The identification and evaluation of a range of business continuity options enables the organization to choose appropriate ways of preventing disruption of its prioritized activities and dealing with any disruptions that take place. Selected options will provide for the resumption of activities:

— at an acceptable level of operation; and

— within an acceptable timeframes.

NOTE The chosen options need to take into account any resilience and countermeasures that are already in place within the organization (see Clause 8.3.3 Protection and mitigation).

e) **Developing and implementing a business continuity response** (see Clause 8.4 Establish and implement business continuity procedures)

Implementing business continuity arrangements results in the creation of an incident response structure (see 8.4.2), the means for detecting and responding to an incident (see 8.4.3 Warning and communication), business continuity plans (see 8.4.4) and other pre-requisites for coping with incidents (see 8.4.5 Recovery).

f) **Exercise and testing** (see Clause 8.5 Exercising and testing)

Exercising and testing provide the opportunity for the organization to ensure that:

— its business continuity capabilities and procedures are complete, current and appropriate; and

— opportunities to improve its business continuity capability are identified.

The programme should be implemented by a responsible person nominated by top management. The programme should address:

— managing the BCM environment;

— managing the business continuity capability; and

— measuring effectiveness.

8.1.2 Managing the BCM environment

Effective management of the BCM environment includes:

g) Ensuring the continuing relevance of the scope, roles and responsibilities for business continuity;

h) Promoting and embedding continuity across the organization and wider, where appropriate;

i) Managing costs associated with the business continuity capability;

j) Establishing and monitoring change management and succession management regimes within the business continuity management system;

k) Arranging or providing appropriate training for staff; and

l) Maintaining programme documentation appropriate to the size and complexity of the organization.

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

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

8.1.3 Managing the business continuity capability

Managing an effective business continuity capability includes:

m) Keeping the business continuity programme current through good practice;

n) Administering the exercise programme;

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

p) Ensuring the maintenance of response documentation appropriate to the needs of the response teams.

8.1.4 Measuring effectiveness

Measuring effectiveness needs to address both:

a) Monitoring the performance of the business continuity capability; and

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

8.1.5 Outcomes

Outcomes indicative of an effective business continuity programme may include the following:

a) Key products and services are identified and protected, ensuring their continuity;

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

c) 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;

d) Regular exercising ensures that staff are trained to respond effectively to an incident or disruption;

e) Requirements of interested parties are understood and able to be delivered;

f) Staff receive adequate support and communications in the event of a disruption;

g) The organization's supply chain is secured;

h) The organization's reputation is protected;

i) The organization remains compliant with its legal and regulatory obligations; and

j) Financial controls are maintained throughout an incident.

8.2 Business impact analysis and risk assessment

8.2.1 General

The organization should establish, implement and maintain a formal and documented process for business impact analysis and risk assessment.

The process should:

a) establish the context of assessment, define criteria and evaluate the potential impact related to a disruptive incident;

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

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

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

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

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

NOTE It is recognized that there are various methodologies for business impact analysis and risk assessment that may be used to determine the order in which these will be conducted.

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

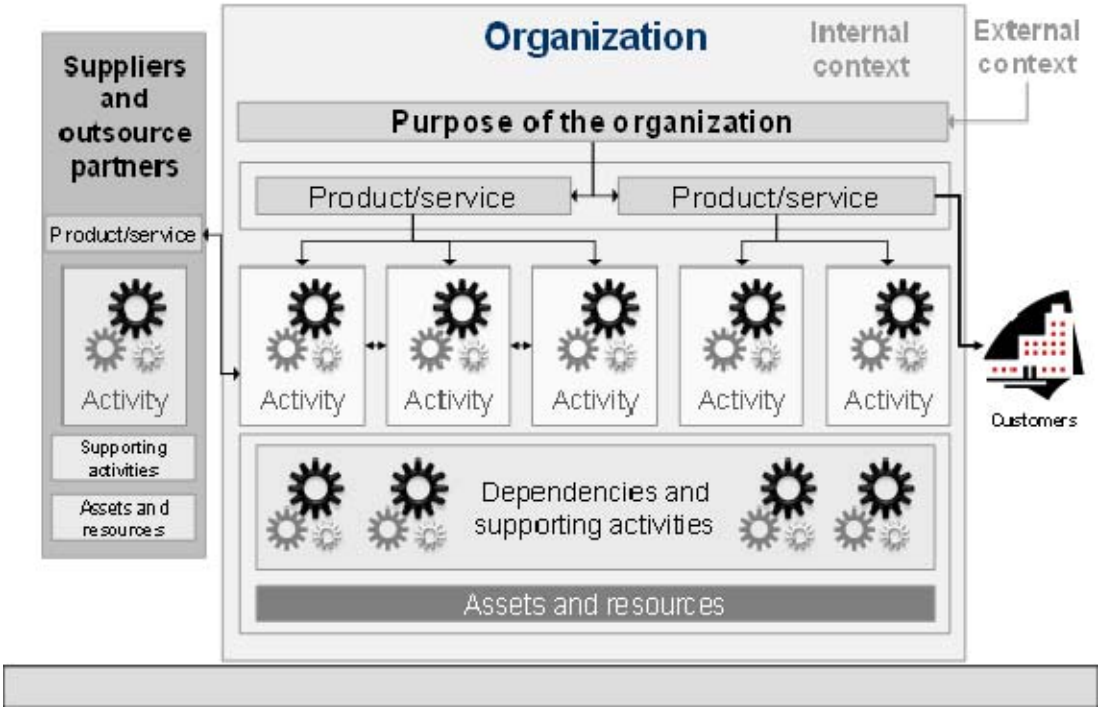

Figure 6 — Understanding the organization

Through understanding, the organization is able to ensure that its business continuity programme aligns with its purpose, statutory duties and obligations to its interested parties. Understanding is achieved through the processes of business impact analysis and risk assessment. This process provides the information required to determine and select business continuity options as described in section 8.3.

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

a) limit the impact of a disruption on the organization's key services;

b) shorten the period of disruption; and

c) reduce the likelihood of a disruption.

The context and evaluation criteria and the format of the outcome of these two processes should be defined and agreed in advance.

The information collected during these processes should be regularly reviewed, particularly during periods of change.

8.2.2 Business impact analysis

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

The purpose of the BIA is to:

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

— determine priorities and timeframes for resumption following an interruption;

— determine appropriate timeframes within which resumption must be achieved in order to maintain the organization's ability to achieve its operational objectives, taking into consideration all contractual, regulatory and statutory requirements;

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

— identify dependencies (both internal and external) relied on to achieve the organization's operational objectives.

The business impact analysis should include:

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

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

   1) Adverse effects on staff or public wellbeing,

   2) Consequences of breaching statutory duties or regulatory requirements,

   3) Damage to reputation,

   4) Reduced financial viability,

   5) Deterioration of product or service quality, and

   6) Environmental damage;

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

NOTE 2 Consideration should be given to daily variations and the cyclical nature of many activities, which may include seasonal variations and association with weekly, monthly or annual deadlines or project delivery dates. The assumption should be made that the disruption occurs at the worst time during these cycles.

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

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

NOTE 4 The time it would take for impacts to become unacceptable may be referred to as 'maximum tolerable period of disruption', 'maximum tolerable period' or 'maximum acceptable outage'.

d) Based on the assessment and taking into account other relevant factors, setting prioritized timeframes for resuming, at a specified minimum acceptable level, the organization's activities; and

e) Taking into account the prioritized timeframes, identifying relevant dependencies and supporting resources, including suppliers, outsource partners and other interested parties

The organization should document its approach to assessing the impact of disruptions over time and its findings and conclusions, including identification of activities, recommended recovery priorities generated from the analysis and significant dependencies.

Information for the business impact analysis may come from:

— interviews;

— questionnaires;

— workshops; and

— other internal and external sources.

8.2.3 Risk assessment

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

ISO 31010 states that 'Risk assessment is that part of risk management which provides a structured process that identifies how objectives may be affected, and analyses the risk in term of consequences and their probabilities before deciding on whether further treatment is required.

Risk assessment attempts to answer the following fundamental questions:

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

b) What are the consequences?

c) What is the probability of their future occurrence? and

d) Are there any factors that mitigate the consequence of the risk or that reduce the probability of the risk?'

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

The organization should understand the threats to and vulnerabilities of each resource required for each activity, and in particular those:

— Required by activities with high priority; or

— With a significant replacement lead-time

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

— Determination of the criteria for risk acceptance: The organization should describe the circumstances under which it is willing to accept risks;

— Identification of acceptable levels of risk: Whatever risk assessment approach is chosen, the organization should identify the levels of risk that it considers acceptable;

— Analysis of the risks: The organization's risk assessment approach should address the following concepts:

  — Specific threats may be described as events or actions which could, at some point, cause an impact to the resources, e.g. threats such as fire, flood, power failure, staff loss, staff absenteeism, computer viruses and hardware failure; and

  — Vulnerabilities might occur as weaknesses within the resources and may, at some point be exploited by the threats, e.g. single points of failure, inadequacies in fire protection, electrical resilience, staffing levels, IT security and IT resilience.

NOTE It may be beneficial to consult **risk registers** that have already been established elsewhere in the organization or by external bodies.

The estimation of a risk to an activity as ‘unlikely’ should not be used to exclude that activity from requiring a continuity strategy. Where the costs of continuity strategies are likely to be prohibitive, the product or service should be removed from the scope of the BCMS.

8.3 Business continuity strategy

8.3.1 Determination and selection

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

The aim of business continuity strategy is to reduce the overall impact of disruptions by shortening the period of interruption and reducing its intensity to acceptable levels.

The organization should determine appropriate strategy options for:

a) Protecting prioritized activities.

   These may be targeted at:

   1) Removing the risk to the activity;

   2) Transferring the activity to a third party (though the responsibility remains with the organization); and

   3) Ceasing or changing the activity if viable alternatives are available.

   Options for protecting prioritized activities should be selected according to:

   4) the perceived vulnerabilities of the activity;

5) the cost of the measures compared to the estimated benefits;

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

7) the overall feasibility and suitability of the option.

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

Continuity options may include:

1) 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;

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

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

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

5) Temporary workaround: Some activities may adopt a different way of working which provides the 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, workaround should only be considered to extend the period before a return to normal is required; and

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

c) Mitigating, responding to and managing impacts.

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

1) Insurance: Purchase of insurance may provide some financial recompense for some losses, but will not meet all costs (e.g. uninsured events, brand, reputation, interested parties value, market share and human consequences). A financial settlement alone will not fully protect the organization and satisfy interested parties expectations. Insurance cover is more likely to be used in conjunction with one or more other strategies; and

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

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

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

The determination of strategy options should include the setting of prioritized time frames for the resumption of activities before the impacts resulting from not resuming them become unacceptable.

Recovery time objectives should be set for each product, service and activity. The recovery time objective should be less than the time within which the impacts of not resuming the product, service or activity would

become unacceptable (as determined during the business impact analysis referred to in 8.2.2). Setting of the recovery time objective may also take into account:

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

— Workarounds (such as manual processes) which may defer the need for full recovery of the activity;

— The dependencies of interrelated activities;

— Complexity or scale of recovery;

— Backlogs and recovery of lost data; and

— Complexity of recovery requirements or need for specialist equipment with a long lead time

8.3.2 Establishing resource requirements

8.3.2.1 General

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

The organization should establish:

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

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

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

   1) Ensure that fiscal decisions may be expedited; and

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

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

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

Resources and their allocation should be reviewed periodically, and in conjunction with top management, to ensure their adequacy. In evaluating the adequacy of resources, consideration should be given to planned changes including and any new facilities, projects, or change in operations.

The organization should choose and implement appropriate continuity strategies to obtain and operate the resources that will be needed for the recovery of its prioritized activities.

A timeline for the recovery of activities and provision of required resources should be prepared in order to define the parameters for the selection of appropriate strategy options.

8.3.2.2 People

The organization should identify appropriate measures to maintain and widen the availability of core skills and knowledge in the event that the incident results in the reduction of staff availability. These measures should

include employees, contractors and other interested parties who possess extensive specialist skills and knowledge. Techniques to protect or enhance those skills may include:

— Documentation of the process in which activities are performed;

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

— Multi-skill training of staff and contractors;

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

— Use of third parties;

— Succession planning; and

— Knowledge retention and management.

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

— Transportation of staff to another location;

— Staff needs at the alternate site such as:

  — Accommodation;

  — Catering facilities;

  — Disruption to normal arrangements, such as child care; and

  — Training on different equipment;

— Challenges posed by home working.

Specialist roles may include:

— Security;

— Transportation logistics; and

— Welfare and emergency

8.3.2.3 Information and data

Information vital to the organization's operation should be protected and recoverable according to the timeframes identified within the BIA.

NOTE 1 Further guidance is given in ISO/IEC 27001. The storage and recovery of such information has to be compliant with relevant legislation.

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

— Confidentiality - for example if the activity is moved to another location;

— Integrity - that the information is reliable and may be trusted;

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

— Currency - as up to date as required to enable the activity to operate - though data lost due the incident may need to be recreated.

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

Information strategies should extend to include:

— Physical (hardcopy) formats; and

— Virtual (electronic) formats, etc.

NOTE 2 In all cases, information needs to be recovered to a point in time that is known and agreed by top management. Various methods of copying may be used, such as electronic or tape backups, microfiche, photocopies, creating dual copies at the time of production and so on. This known recovery point is often referred to as the 'recovery point objective'.

NOTE 3 The location where copies of data is stored should be located at a sufficient distance to ensure that the incident does not compromise its integrity or access. However the ideal separation distance may compromise the timely availability of the data. This limitation should be agreed and documented.

The required currency of information available after a disruption should also be documented – this may be obtained using the recovery point objective of each category of information.

Information specific to BCM may include:

— Contact information;

— Supplier, interested parties and interested party details;

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

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

8.3.2.4 Buildings, work environment and associated utilities

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

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

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

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

c) Emergency control centres;

d) Alternative premises provided by third-party specialists;

e) Working from home or at remote sites;

f) Other agreed suitable premises; and

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

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

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

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

It may be appropriate to move the workload rather than the staff, e.g. a manufacturing line or a call centre's workload.

This may require spare capacity at the alternate site or additional (whether by overtime or recruitment) and other resources available to operate the activity

8.3.2.5 Facilities, equipment and consumables

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

Key facilities and machinery required by an activity may become a bottleneck for its resumption because of difficulties of replacement or long lead time. Business continuity options to resolve such a bottle neck needs longer term planning as management decision.

Techniques for providing these may include:

— Storage of additional supplies at another location;

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

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

— Holding of materials at warehouses or shipping sites;

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

— Identification of alternative/substitute supplies; and

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

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

— Increasing the number of suppliers;

— Encouraging or requiring suppliers to have a validated business continuity capability;

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

— The identification of alternative, capable suppliers.

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

8.3.2.6 Information communications technology (ICT) systems

Specific techniques ought to be developed to safeguard, replace or restore specialized or custom built technologies with long lead times. The organization may need to make provision for manual operations before full technology services are recovered.

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

— Provision made within the organization;

— Services delivered to the organization; and

— Services provided externally by a third party.

Technology techniques may include:

— Geographical spread of technology, i.e. maintaining the same technology at different locations that will not be affected by the same business disruption;

— Holding older equipment as emergency replacement or spares; and

— Additional risk mitigation for unique or long lead time equipment.

Information technology (IT) services frequently need complex continuity techniques. Where such techniques are required, consideration should be given to:

— Recovery time objectives (RTOs) for systems and applications which enable the recovery time objective of each activities to be achieved;

— Location and distance between technology sites;

— Number of technology sites;

— Remote access;

— The use of un-staffed (dark) sites as opposed to staffed sites;

— Telecoms connectivity and redundant routing;

— The nature of ‘failover’ (whether manual intervention is required to activate alternative IT provision or whether this needs to occur automatically); and

— Third-party connectivity and external links.

If a technique of ‘failing over’ from one site to another is adopted, the network path distance between the two sites has to be carefully considered as the distance between the sites could have a negative impact on the way in which IT systems operate.

Where more than one site hosts an organization's IT, there may be a mutual IT recovery strategy, so that the systems, network and storage at each site is sized to cope with the combined traffic and work of the other(s) in addition to its own work.

Another solution to relocating people to alternative premises is to provide them with remote access to IT via dial-up, or through the Internet using Virtual Private Network (VPN) or similar technology.

NOTE Further guidance on continuity for IT and telecommunications hardware may be found in such documents as ISO/IEC 27031, ISO/IEC 27001 and ISO/IEC 20000 (both parts).

8.3.2.7 Transportation

Transportation may need to be provided after an incident for:

— Staff sent home if normal means of transport is unavailable;

— Staff relocated to alternative work location; and

Resources may be need to be transferred to an alternative site.

If logistic arrangements for incoming supplies and outgoing deliveries of products and services are disrupted, alternative logistic options should be selected. Techniques for providing these may include:

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

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

Entering into support agreements with business partners and other interested parties.

8.3.2.8 Finance

Financial controls must be maintained through an incident. This may include:

— Availability of funds for emergency purchases required for response and recovery; and

— Recording of expenses during an incident.

8.3.2.9 Partners and suppliers

If a product, service or activity has been outsourced, the risk accountability for that product, service or activity remains vested within the organization. Consequently, an organization should assure itself that its key suppliers or outsource partners have effective continuity arrangements in place. One method of doing this is to obtain audited evidence of the viability of key suppliers' continuity plans and their exercising and maintenance programmes.

8.3.3 Protection and mitigation

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

8.4 Establish and implement business continuity procedures

8.4.1 General

The organization should provide appropriate procedures to manage disruptive incidents and ensure that its activities continue based on their identified recovery objectives. These procedures should also cover the activities required to manage a disruptive incident. The business continuity procedures should establish the appropriate internal and external communications protocol and be:

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

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

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

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

8.4.2 Incident response structure

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

The response structure should provide for:

— Identifying impact thresholds that justify initiation of formal response;

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

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

— Initiating an appropriate business continuity response;

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

— Resources being available to support the processes and procedures needed to manage a disruptive incident or work to minimize impact before realized; and

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

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

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

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

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

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

Each team should have procedures for managing an incident according to its responsibilities.

8.4.3 Warning and communication

8.4.3.1 General

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

a) detecting an incident and alerting response personnel;

b) continuing monitoring of incident;

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

d) external communications with partner organizations and other interested parties;

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

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

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

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

i) facilitating structured communication with emergency responders;

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

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

l) operations of a communications facility.

The organization should decide, using life safety as the first priority and in consultation with its interested parties, whether to communicate externally about its significant risks and impacts. Special arrangements may be required for ensuring the effectiveness of communication with interested parties with specific needs, such as disability. This decision should be documented.

If the decision is to communicate then the organization should establish and implement procedures for warnings, alerts and external communication, including, as appropriate, the media.

The warning and communication system should be regularly exercised.

8.4.3.2 Incident response procedures

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

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

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

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

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

— structured communication with emergency responders;

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

— provide communication between the various response teams with the organization;

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

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

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

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

8.4.3.3 Incident response facilities

These procedures may be facilitated by the use a dedicated or ad hoc communications facility. This should be located sufficiently far from the affected site that its operation is not impeded by the incident.

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

— Loud-hailers or public address systems;

— Spare mobile phones; and

— Two-way radios.

8.4.4 Business continuity plans

8.4.4.1 General

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

These procedures should address all aspects of responding to an incident with particular regard to life safety issues and address all those who will need to be involved in the response.

Timescales and performance levels should be based on the information gathered during the business impact analysis (referred to in 8.2.2) and the business continuity strategy selected (referred to in 8.3).

The following should be clearly identifiable within each plan:

— Purpose and scope;

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

— Activation criteria and procedures;

— Implementation procedures;

— Roles, responsibilities, and authorities;

— Communication requirements and procedures;

— Internal and external interdependencies and interactions;

— Resource requirements; and

— Information flow and documentation processes.

Following commencement of a potentially disruptive incident, there are a range of actions that should be considered in order to determine whether and when to activate and deploy the plan(s), including:

a) responding to and assessing the incident:

   1) What happened and how did it occur?

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

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

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

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

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

d) mobilizing the incident response personnel in teams for stabilization, continuity and recovery activities;

e) establishing and running the incident management location;

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

g) controlling and coordinating all activated procedures;

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

i) monitoring the incident as it progresses;

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

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

l) conducting a debrief and identifying learning opportunities; and

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

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

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

— be sufficiently reliable.

This may be achieved by:

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

— contracts, agreements or service levels with third parties.

The operation of the procedure will not be affected by the same disruption that invoked the procedure - in case of pandemic, for example, by ensuring its physical, technical and personnel separation. However total separation for all scales and types of incident is not possible and this limitation should be identified and

agreed with top management. This limitation could be expressed in terms of distance, minimum personnel or severity and may be determined by the response of civil authorities to a severe and/or widespread incident.

8.4.4.2 Guidance on content of business continuity plans

A small organization may have a single documented procedure that encompasses all requirements and covers its entire operations. A very large organization may have many documented procedures, each with a defined purpose and scope.

The purpose and scope of procedure should be defined, agreed by top management, and understood by those who will put it into effect. Any relationship to other relevant business continuity procedures or documents within the organization should be clearly referenced and the method of obtaining and accessing them described.

All business continuity procedures should be concise and accessible to those with responsibilities defined within them. Collectively, all business continuity procedures should contain the following elements:

a) Document controls (see 7.5.3)

b) Roles and responsibilities:

   1) There should be defined roles and responsibilities for individuals or the team who will use the response procedure during and following an incident; and

   2) There should be guidelines and criteria regarding which individuals have the authority to invoke the procedures and under what circumstances – this may follow defined escalation stages (for example World Health Organization guidance on pandemics.

c) Invocation and standing down:

   1) Each response procedure should have a method by which it is invoked with consideration as to whether this is within or outside normal working hours;

   2) Each response procedure should contain a formal means of standing the team down; and

   3) Each response procedure should as appropriate identify meeting locations with alternatives.

d) Incident management:

   1) The response procedure should contain details of actions and tasks that need to be performed;

   2) Where appropriate the response procedure should include management of welfare issues of affected personnel and the welfare of the team members;

   3) The response procedure should address issues at the appropriate level - strategic, tactical or operational options. Issues that are at other levels should be escalated or delegated to other teams as required; and

   4) The response procedure should specify a method for recording key information about the incident, actions taken and decisions made.

e) Contact information:

   1) The response procedure should contain contact details for interested parties relevant that are relevant to it – contact details must be held with regard to local Data Protection legislation; and

   2) Business continuity procedures should contain contact and mobilization details for any relevant agencies, organizations and resources that might be required to support the response.

f) Communication:

1) All business continuity procedures should address communication with other teams.

8.4.4.3 Specific types of procedures

8.4.4.3.1 Incident management / strategic management procedures

The purpose of an Incident Management procedure is to allow the organization's top management to take control during the initial phase of an incident when its reputation is most likely to be threatened.

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

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

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

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

— Space for the required number of people;

— Effective primary and secondary means of communication; and

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

Other response teams may require similar facilities.

8.4.4.3.2 Communications procedures

Communications procedures may be included in the incident management response procedure or a separate communications response procedure (and team) may be appropriate.

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

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

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

1) the incident communications strategy;

2) preferred interface with the media;

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

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

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

It may be appropriate to:

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

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

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

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

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

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

8.4.4.3.3 Incident and welfare procedures

Incident and welfare procedures cover the initial stage of an incident involving damage or threat to safety. They should contain tasks and information to manage the immediate consequences of a disruption including:

— the welfare of individuals; and

— strategic and operational options for responding to the disruption; and prevention of further loss or unavailability of activities.

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

A welfare response procedure should include:

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

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

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

They may also include:

— Translation services;

— Transport assistance including directions as required;

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

— Locating displaced workforce or contractors;

— Managing telephone help lines; and

— Rehabilitation and counseling services (physical and emotional).

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

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

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

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

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

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

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

— Emergency power production (generators);

— Communications systems;

— Food and water;

— Technical information;

— Clothing and shelter;

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

— Specialized volunteer groups (e.g., red cross, amateur radio, religious relief organizations, charitable agencies;

— Volunteer, community, and emergency response support; and

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

One or more procedures should be prepared to address the minimization of loss of resources after a destructive incident. This may include guidance on:

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

— Security of the premises once handed over by the Emergency Services.

8.4.4.3.4 Procedures for resuming activities

Each procedure should specify the:

— Prioritized activities to be resumed;

— Timescales within which they are to be resumed;

— Recovery levels needed for each prioritized activity; and

— Situations in which the procedure may be utilized.

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

— Resource numbers;

— Skills and qualifications;

— Technical equipment;

— Telecommunications facilities; and

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

In the event that lack of a service or resource makes the activity response procedure's objectives unachievable, escalation actions should be defined. These actions may include:

— Mobilization of external and third-party resources;

— Communication of recovery actions; and

— Procedures for implementing manual workarounds, system recovery, etc.

Resource requirements should be documented and may include:

— Vital records (hardcopy and electronic);

— Operating and procedure manuals;

— IT technical recovery plans and procedures;

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

— Alternate office and operation locations (if required);

— Authorities/delegations for the payment of emergency expenses;

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

— IT infrastructure and applications documentation;

— Telecommunications support source;

— Office and specialist equipment sources; and

— Utilities (water, power etc.) contacts.

8.4.4.3.5 Recovery of information communications technology (ICT) systems

The procedures for resuming activities should reference disaster recovery procedures that provide for the recovery of the information communications technology required for resumption of prioritized activities. These disaster recovery procedures should at minimum address:

— The logistical procedures for invoking the disaster recovery procedures and deploying personnel;

— Accessing back-up data and acquiring alternative hardware; and

— Restoration of data and communications.

The disaster recovery procedures should support the timetable of application and communications requirements set out in all business continuity procedures.

8.4.5 Recovery

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

These should also address relevant audit and corporate governance requirements.

Recovery commences once prioritized activities have resumed. Its primary objective is to get operations back to the state they were before the incident. This may be achieved either by repairing the damage resulting from the incident, migrating operations from temporary premises back to the restored primary business location or moving to a new location. A decision on how best to 'return to normal' will need to be taken based on the severity of the damage caused by the incident and estimates of how long it might take to establish the necessary facilities.

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

a) establish recovery resources and infrastructure;

b) operate at recovery facilities;

c) restore damaged facilities;

d) secure emergency procurement and funding;

e) salvage equipment in damaged facilities;

f) make claims against existing insurance policies;

g) obtain additional manpower to support the recovery effort;

h) select options for restoring and returning to business;

i) migrate operations to recovery facilities;

j) recover lost documented information;

k) communicate with relevant interested parties and their respective frequencies;

l) normalize operations at the restored facilities;

m) conduct a post recovery review; and

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

The documented procedures should also make provision for activities that have not been prioritized during the business impact analysis referred to in 8.2.2 . Situations may arise in which facilities suitable for the resumption of such an activity will not be available within its recovery time objective.

8.5 Exercising and testing

8.5.1 General

An organization's business continuity and incident management arrangements cannot be considered reliable until exercised and unless their currency is maintained. Exercising is essential to developing teamwork, competence, confidence and knowledge all of which are vital at the time of an incident.

The organization should exercise its continuity procedures to ensure that they are consistent with business continuity management objectives.

8.5.2 Exercise programme

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

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

An exercise programme should be devised that, over a period of time, leads to objective assurance that the procedures will work as anticipated when required. The programme should:

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

b) Exercise the business continuity arrangements and infrastructure (including roles, responsibilities, and any incident management locations and work areas, etc.); and

c) Validate the technology and telecommunications recovery, including the availability and relocation of staff.

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

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

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

The scope and detail of the exercises should mature through the programme based on the organization's experience, resources, and capabilities. Early tests may include checklists, simple exercises, and small components then the organization may move through table top exercises to full scale live simulations.

8.5.3 Exercising business continuity plans

Exercises are activities designed to examine the staff's ability to effectively respond, recover and continue to perform assigned business functions 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 should have clearly defined objectives which should be agreed and signed off before the commencement of detailed exercise development.

Exercises may:

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

— Allow the organization to develop innovative solutions.

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

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

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

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

a) Improved awareness of the organizational context and priorities;

b) Improved understanding of the content and use of business continuity procedures;

c) Improved confidence in responding to incidents;

d) An opportunity to improve capabilities;

e) An assessment of the utility and applicability of the BCM options;

f) An evaluation of the adequacy of developed capabilities and resource allocations;

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

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

i) Assurance that business continuity procedures are capable of being implemented when required;

j) Improved confidence of interested parties regarding the organization’s preparedness; and

k) A means of fulfilling regulatory, contractual or organizational governance requirements.

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

The principal types of exercise are described in ISO 22398.

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

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

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

Benefits of exercising and testing include:

— validation of planning scope, assumptions and strategies;

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

— assurance of the capacity of the alternate facilities;

— increase efficiency and reduce the time necessary for accomplishment of a process (e.g., using repeated drills to shorten response times); and

— improved awareness and knowledge of interested parties about BCM and their roles.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.1.1 General

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

The procedures for monitoring performance should include:

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

b) Monitoring the extent to which the organization’s business continuity policy, objectives and targets are met;

c) Assessing the performance of the processes, procedures and functions that protect prioritized activities;

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

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

f) Recording data and results of monitoring and measurement sufficient to facilitate subsequent corrective action analysis.

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

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

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

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

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

9.1.2 Evaluation of continuity procedures

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

The evaluations should address the possible need for changes to policy, strategy, objectives and other elements of the business continuity management system in the light of such things as exercise results, changing circumstances and the commitment to continual improvement.

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

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

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

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

c) the organization's business continuity competence and its business continuity capability are effective and fit-for-purpose and will permit management, command, control and coordination of an incident;

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

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

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

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

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

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

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

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

— identify any new products and services and their dependent activities that need to be included in the business continuity management programme;

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

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

NOTE If there are major business changes, the organization should reassess the business impact analysis referred to in 8.2.2. The other components of the business continuity programme may need to be amended to take account of these changes.

The outcomes from the business continuity maintenance process should include:

— documented evidence of the proactive management and governance of the organization's business continuity programme;

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

— verification of the monitoring and control of the business continuity risks faced by the organization; and

— documented evidence that material changes to the organization's structure, products and services, activities, purpose, staff and objectives have been incorporated into the organization's business continuity and procedures.

In the event of an incident that disrupts the organization's prioritized activities or requires a business continuity response, the post-incident review undertaken should:

— identify the nature and cause of the incident;

— assess the adequacy of management's response;

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

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

— identify improvements to be made to the business continuity arrangements

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

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

9.2 Internal audit

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

It is essential to conduct internal audits of the BCMS to ensure that the BCMS is achieving its objectives, that it conforms to its planned arrangements and has been properly implemented and maintained, and to identify opportunities for improvement. Internal audits of the BCMS should be conducted at planned intervals to determine and provide information to top management on appropriateness and effectiveness of the BCMS as well as to provide a basis for setting objectives for continual improvement of BCMS performance.

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

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

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

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

9.3 Management review

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

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

— Policy;

— Resource allocations;

— Risk acceptance;

— Objectives and targets; and

— Business continuity strategies.

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) BIA and risk assessment: The BCMS should be reviewed every time a BIA or risk assessment is completed for the organization. The results of the BIA and risk assessment may be used to determine whether the BCMS adequately address the risks facing the organization.

b) 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;

c) Regulatory requirements: New regulatory requirements may require a review of the BCMS;

d) Incident experience: A review should be performed following a response to a disruptive incident, whether or not the response procedure was activated. If activated, the review should take into account the history of the response procedure, how it worked, why it was activated, etc. If the response procedure was not activated, the review should examine why and whether this was an appropriate decision; and

e) Test and exercise results: Based on test and exercise results, the BCMS should be reviewed and modified as necessary.

Continual improvement and BCMS maintenance should reflect changes in the activities, functions, and risks to the operation of the organization that will affect the management system. The following are examples of procedures, systems, or processes that may affect the BCMS:

— Policy changes;

— Changes to the organization and its business processes;

— Changes in scope of the BCMS;

— Changes in assumptions in BIA and risk assessment;

— Personnel changes (employees and contractors) and their contact information;

— Supplier and supply chain changes;

— Process and technology changes;

— Systems and application software changes;

— Hazards and threat changes;

— Lessons learned from exercising and testing;

— Lessons learned from external organizations' disruptive incidents;

— Issues discovered during the implementation of business continuity procedures;

— Changes to external environment (new businesses in area, new roads or changes to existing traffic patterns, etc.); and

— Other items noted during review of business continuity procedures and identified during the risk assessment and impact analysis.

The output from the management review should include decisions and actions, including the communication of results of management review to interested parties.

10 Improvement

10.1 Nonconformity and corrective action

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

The organization should establish effective procedures to ensure that non-fulfillment of a requirement, planning approach, incidents, near misses (near hits) and weaknesses associated with the BCMS (its capability and business continuity procedures) are identified and communicated in a timely manner to prevent further occurrence of the situation, as well as identify and address root causes. The procedures should enable ongoing detection, analysis and elimination of actual and potential causes of non-conformities.

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

Nonconformities, fixes, corrective actions and continuous improvement are components of a single, interrelated process. Corrective action addresses recurrence of the problem, and the root cause and associated conditions for the occurrence of a problem.

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

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

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

Corrective actions that result in changes to the BCMS should be reflected in the documentation. They should also trigger a revisit of the risk assessment and impact analysis in order to evaluate their effect on business continuity procedures and training needs. Changes should be communicated to all who need to know.

Action required to eliminate the cause of nonconformities should include:

a) reviewing the nonconformities;

b) determining what has caused them;

c) evaluating the need for action to ensure that they do not recur;

d) determining and implementing appropriate action that is needed; and

e) reviewing the effectiveness of the corrective action taken.

The corrective actions taken should be appropriate to the potential and actual effects of the nonconformities encountered and the organization should ensure that any necessary changes are made to the BCMS and retain documented information that provides evidence of:

— the nature of the nonconformity;

— the corrective actions taken; and

— the results of the corrective actions.

The organization should identify and review its changing internal and external context, and identify appropriate action focusing attention on significantly changed risks.

The priority of corrective actions should be determined based on the results of the risk assessment and impact analysis.

10.2 Continual improvement

The organization should continually improve the effectiveness of the BCMS.

Continual improvement is a key element of any management system standard. Continuous improvement may operate at three levels within the PDCA cycle:

a) At the BCMS level, cycle time is a year up to several years;

b) At the business continuity programme level, cycle time may be six months up to one year; and

c) Some elements of the programme may have a cycle time of a few months.

Cycle times may vary between organizations depending on their size, nature and complexity.

Continual improvement should be driven by the business continuity policy, objectives, audit results, analysis of monitored events, corrective actions and management review.

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

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

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

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

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

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

— Determine what changes to implement (corrective action).

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

Bibliography

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

[2] BS 25999-1:2006, *Business continuity management — Code of practice*, BSI British Standards

[3] BS 25999-2:2007, *Business continuity management — Specification,* BSI British Standards

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

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

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

[7] *Business Continuity Plan Drafting Guideline*, Ministry of Economy, Trade and Industry (Japan), 2005

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

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

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

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

[12] Bravener, Lee C. (1999). *The Road to Continuous Improvement. Quality Digest*, May 1999 (http://www.qualitydigest.com/may99/html/body_ci.html)