INTERNATIONAL STANDARD

ISO 22301

First edition
2012-05-15

Corrected version
2012-06-15

Societal security — Business continuity management systems — Requirements

Sécurité sociétale — Gestion de la continuité des affaires — Exigences

Reference number
ISO 22301:2012(E)

Licensed to Leader & Reader Co.,Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012



COPYRIGHT PROTECTED DOCUMENT

© ISO 2012

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

Contents

Page

Foreword ... iv

0 Introduction ... v
0.1 General ... v
0.2 The Plan-Do-Check-Act (PDCA) model ... v
0.3 Components of PDCA in this International Standard ... vi

1 Scope ... 1

2 Normative references ... 1

3 Terms and definitions ... 1

4 Context of the organization ... 8
4.1 Understanding of the organization and its context ... 8
4.2 Understanding the needs and expectations of interested parties ... 9
4.3 Determining the scope of the business continuity management system ... 9
4.4 Business continuity management system ... 10

5 Leadership ... 10
5.1 Leadership and commitment ... 10
5.2 Management commitment ... 10
5.3 Policy ... 11
5.4 Organizational roles, responsibilities and authorities ... 11

6 Planning ... 12
6.1 Actions to address risks and opportunities ... 12
6.2 Business continuity objectives and plans to achieve them ... 12

7 Support ... 12
7.1 Resources ... 12
7.2 Competence ... 13
7.3 Awareness ... 13
7.4 Communication ... 13
7.5 Documented information ... 14

8 Operation ... 15
8.1 Operational planning and control ... 15
8.2 Business impact analysis and risk assessment ... 15
8.3 Business continuity strategy ... 16
8.4 Establish and implement business continuity procedures ... 17
8.5 Exercising and testing ... 19

9 Performance evaluation ... 19
9.1 Monitoring, measurement, analysis and evaluation ... 19
9.2 Internal audit ... 20
9.3 Management review ... 21

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

Bibliography ... 24

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

Foreword

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

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

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

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

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

This corrected version of ISO 22301:2012 incorporates the following corrections:

— first list in 6.1 changed from a numbered to an unnumbered list;

— commas added at the end of list items in 7.5.3 and 8.3.2;

— bibliography items [19] and [20] separated, which were merged in the original;

— font size adjusted in several places.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

0 Introduction

0.1 General

This International Standard specifies requirements 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 capability to manage disruptive incidents,

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

— continual improvement based on objective measurement.

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

a) a policy;

b) people with defined responsibilities;

c) management processes relating to

   1) policy,

   2) planning,

   3) implementation and operation,

   4) performance assessment,

   5) management review, and

   6) improvement;

d) 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 impact of the organization's environment on the organization and therefore other organizations may need to be involved in the recovery process.

0.2 The Plan-Do-Check-Act (PDCA) model

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

This ensures a degree of consistency with other management systems standards, such as ISO 9001 *Quality management systems*, ISO 14001, *Environmental management systems*, ISO/IEC 27001, *Information security management systems*, ISO/IEC 20000-1, *Information technology — Service management*, and ISO 28000, *Specification for security management systems for the supply chain*, thereby supporting consistent and integrated implementation and operation with related management systems.

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

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

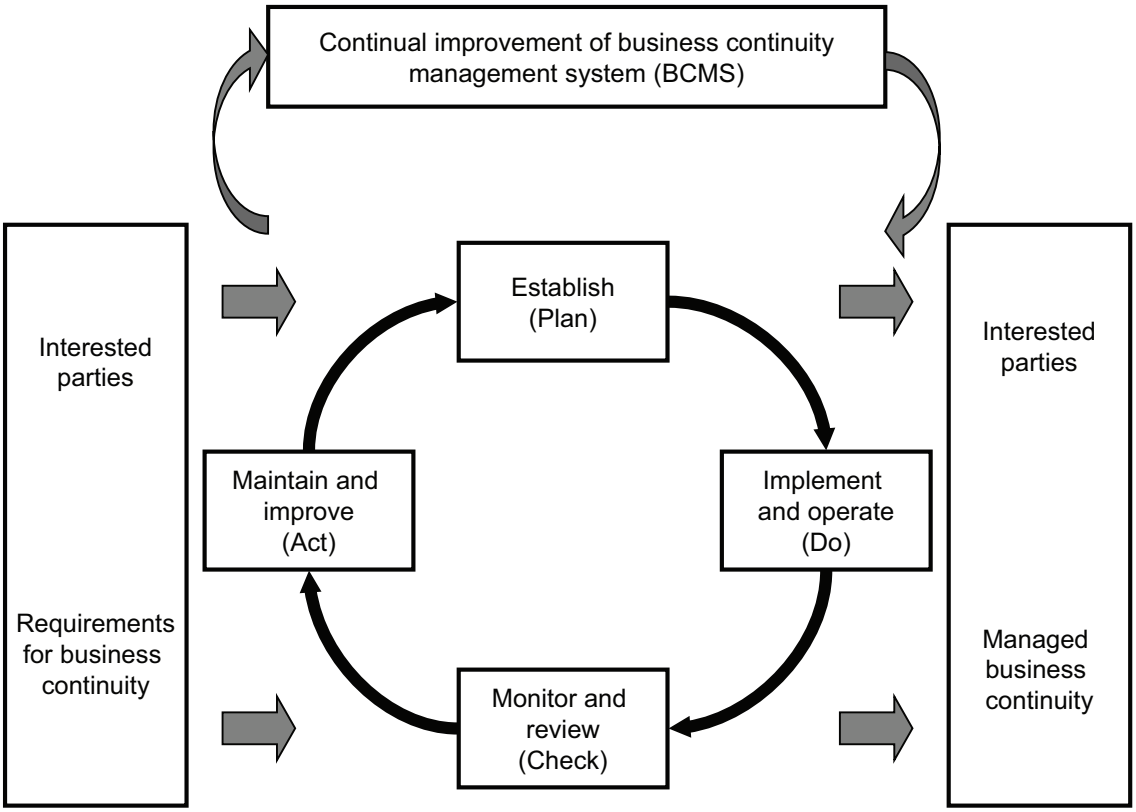

Figure 1 — PDCA model applied to BCMS processes

Table 1 — Explanation of PDCA model

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 policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the BCMS by taking corrective action, based on the results of management review and reappraising the scope of the BCMS and business continuity policy and objectives.

0.3 Components of PDCA in this International Standard

In the Plan-Do-Check-Act model as shown in Table 1, Clause 4 through Clause 10 in this International Standard cover the following components.

— Clause 4 is a component of Plan. It introduces requirements necessary to establish the context of the BCMS as it applies to the organization, as well as needs, requirements, and scope.

— Clause 5 is a component of Plan. It summarizes the requirements specific to top management's role in the BCMS, and how leadership articulates its expectations to the organization via a policy statement.

— Clause 6 is a component of Plan. It describes requirements as it relates to establishing strategic objectives and guiding principles for the BCMS as a whole. The content of Clause 6 differs from establishing risk treatment opportunities stemming from risk assessment, as well as business impact analysis (BIA) derived recovery objectives.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

NOTE The business impact analysis and risk assessment process requirements are detailed in Clause 8.

— Clause 7 is a component of Plan. It supports BCMS operations as they relate to establishing competence and communication on a recurring/as-needed basis with interested parties, while documenting, controlling, maintaining and retaining required documentation.

— Clause 8 is a component of Do. It defines business continuity requirements, determines how to address them and develops the procedures to manage a disruptive incident.

— Clause 9 is a component of Check. It summarizes requirements necessary to measure business continuity management performance, BCMS compliance with this International Standard and management's expectations, and seeks feedback from management regarding expectations.

— Clause 10 is a component of Act. It identifies and acts on BCMS non-conformance through corrective action.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

Societal security — Business continuity management systems — Requirements

1 Scope

This International Standard for business continuity management specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.

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

It is not the intent of this International Standard to imply uniformity in the structure of a Business Continuity Management System (BCMS), but for an organization to design a BCMS that is appropriate to its needs and that meets its interested parties' requirements. 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 applicable to all types and sizes of organizations that wish to

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

b) ensure conformity with stated business continuity policy,

c) demonstrate conformity to others,

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

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

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

2 Normative references

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

There are no normative references.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

EXAMPLE Such processes include accounts, call centre, IT, manufacture, distribution.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

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 can be an internal audit (first party) or an external audit (second party or third party), and it can 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
capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incident

[SOURCE: ISO 22300]

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

3.5
business continuity management system
BCMS
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 actitivites and the effect that a business disruption might have upon them

[SOURCE: ISO 22300]

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

3.10
conformity
fulfilment of a requirement

[SOURCE: ISO 22300]

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

3.11
continual improvement
recurring activity to enhance performance

[SOURCE: ISO 22300]

3.12
correction
action to eliminate a detected nonconformity

[SOURCE: ISO 22300]

3.13
corrective action
action to eliminate the cause of a nonconformity and to prevent recurrence

NOTE In the case of other undesirable outcomes, action is necessary to minimize or eliminate causes and to reduce impact or prevent recurrence. Such actions fall outside the concept of “corrective action” in the sense of this definition.

[SOURCE: ISO 22300]

3.14
document
information and its supporting medium

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

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

3.15
documented information
information required to be controlled and maintained by an organization and the medium on which it is contained

NOTE 1 Documented information can be in any format and on any media from any source.

NOTE 2 Documented information can refer to

— the management system, including related processes;

— information created in order for the organization to operate (documentation);

— evidence of results achieved (records).

3.16
effectiveness
extent to which planned activities are realized and planned results achieved

[SOURCE: ISO 22300]

3.17
event
occurrence or change of a particular set of circumstances

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

NOTE 2 An event can consist of something not happening.

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

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

[SOURCE: ISO/IEC Guide 73]

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

3.18
exercise
process to train for, assess, practice, and improve performance in an organization

NOTE 1 Exercises can be used for: validating policies, plans, procedures, training, equipment, and inter-organizational agreements; clarifying and training personnel in roles and responsibilities; improving inter-organizational coordination and communications; identifying gaps in resources; improving individual performance; and identifying opportunities for improvement, and controlled opportunity to practice improvisation.

NOTE 2 A test is a unique and particular type of exercise, which incorporates an expectation of a pass or fail element within the goal or objectives of the exercise being planned.

[SOURCE: ISO 22300]

3.19
incident
situation that might be, or could lead to, a disruption, loss, emergency or crisis

[SOURCE: ISO 22300]

3.20
infrastructure
system of facilities, equipment and services needed for the operation of an organization

3.21
interested party
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

NOTE This can be an individual or group that has an interest in any decision or activity of an organization.

3.22
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 can be demonstrated by the freedom from responsibility for the activity being audited.

3.23
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

3.24
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 can 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 can 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.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

3.25
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.

3.26
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.

3.27
measurement
process to determine a value

3.28
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

3.29
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.

3.30
mutual aid agreement
pre-arranged understanding between two or more entities to render assistance to each other

[SOURCE: ISO 22300]

3.31
nonconformity
non-fulfilment of a requirement

[SOURCE: ISO 22300]

3.32
objective
result to be achieved

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

NOTE 2 Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels [such as strategic, organization-wide, project, product and process).

NOTE 3 An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a societal security objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

NOTE 4 In the context of societal security management systems standards, societal security objectives are set by the organization, consistent with the societal security policy, to achieve specific results.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

3.33
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, sole-trader, company, corporation, firm, enterprise, authority, partnership, 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 operating unit can be defined as an organization.

3.34
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.

3.35
performance
measurable result

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

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

3.36
performance evaluation
process of determining measurable results

3.37
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.

3.38
policy
intentions and direction of an organization as formally expressed by its top management

3.39
procedure
specified way to carry out an activity or a process

3.40
process
set of interrelated or interacting activities which transforms inputs into outputs

3.41
products and services
beneficial outcomes provided by an organization to its customers, recipients and interested parties, e.g. manufactured items, car insurance and community nursing

3.42
prioritized activities
activities to which 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]

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

3.43
record
statement of results achieved or evidence of activities performed

3.44
recovery point objective
RPO
point to which information used by an activity must be restored to enable the activity to operate on resumption

NOTE Can also be referred to as “maximum data loss”.

3.45
recovery time objective
RTO
period of time following an incident within which

— product or service must be resumed, or

— 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.

3.46
requirement
need or expectation that is stated, generally implied or obligatory

NOTE 1 “Generally implied” means that it is a customary or common practice for the organization and interested parties that the need or expectation under consideration is implied.

NOTE 2 A specified requirement is one that is stated, for example in documented information.

3.47
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

3.48
risk
effect of uncertainty on objectives

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

NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). An objective can 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 deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

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.

[SOURCE: ISO/IEC Guide 73]

3.49
risk appetite
amount and type of risk that an organization is willing to pursue or retain

3.50
risk assessment
overall process of risk identification, risk analysis and risk evaluation

[SOURCE: ISO Guide 73]

3.51
risk management
coordinated activities to direct and control an organization with regard to risk

[SOURCE: ISO Guide 73]

3.52
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.

[SOURCE: ISO 22300]

3.53
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 If the scope of the management system covers only part of an organization then top management refers to those who direct and control that part of the organization.

3.54
verification
confirmation, through the provision of evidence, that specified requirements have been fulfilled

3.55
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 shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its BCMS.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

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

The organization shall identify and document the following:

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

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

c) the organization's risk appetite.

In establishing the context, the organization shall

1) articulate its objectives, including those concerned with business continuity,

2) define the external and internal factors that create the uncertainty that gives rise to risk,

3) set risk criteria taking into account the risk appetite, and

4) define the purpose of the BCMS.

4.2 Understanding the needs and expectations of interested parties

4.2.1 General

When establishing its BCMS, the organization shall determine

a) the interested parties that are relevant to the BCMS, and

b) the requirements of these interested parties (i.e. their needs and expectations whether stated, generally implied or obligatory).

4.2.2 Legal and regulatory requirements

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

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

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

4.3 Determining the scope of the business continuity management system

4.3.1 General

The organization shall determine the boundaries and applicability of the BCMS to establish its scope.

When determining this scope, the organization shall consider

— the external and internal issues referred to in 4.1, and

— the requirements referred to in 4.2.

The scope shall be available as documented information.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

4.3.2 Scope of the BCMS

The organization shall

a) establish the parts of the organization to be included in the BCMS,

b) establish BCMS requirements, considering the organization's mission, goals, internal and external obligations (including those related to interested parties), and legal and regulatory responsibilities,

c) identify products and services and all related activities within the scope of the BCMS,

d) take into account interested parties' needs and interests, such as customers, investors, shareholders, the supply chain, public and/or community input and needs, expectations and interests (as appropriate), and

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

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

4.4 Business continuity management system

The organization shall establish, implement, maintain and continually improve a BCMS, including the processes needed and their interactions, in accordance with the requirements of this International Standard.

5 Leadership

5.1 Leadership and commitment

Persons in top management and other relevant management roles throughout the organization shall demonstrate leadership with respect to the BCMS.

EXAMPLE This leadership and commitment can be shown by motivating and empowering persons to contribute to the effectiveness of the BCMS.

5.2 Management commitment

Top management shall demonstrate leadership and commitment with respect to the BCMS by

— ensuring that policies and objectives are established for the business continuity management system and are compatible with the strategic direction of the organization,

— ensuring the integration of the business continuity management system requirements into the organization's business processes,

— ensuring that the resources needed for the business continuity management system are available,

— communicating the importance of effective business continuity management and conforming to the BCMS requirements,

— ensuring that the BCMS achieves its intended outcome(s),

— directing and supporting persons to contribute to the effectiveness of the BCMS,

— promoting continual improvement, and

— supporting other relevant management roles to demonstrate their leadership and commitment as it applies to their areas of responsibility.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

NOTE 1 Reference to “business” in this International Standard is intended to be interpreted broadly to mean those activities that are core to the purposes of the organization’s existence.

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

— establishing a business continuity policy,

— ensuring that BCMS objectives and plans are established,

— establishing roles, responsibilities, and competencies for business continuity management, and

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

NOTE 2 These persons can hold other responsibilities within the organization.

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

— defining the criteria for accepting risks and the acceptable levels of risk,

— actively engaging in exercising and testing,

— ensuring that internal audits of the BCMS are conducted,

— conducting management reviews of the BCMS, and

— demonstrating its commitment to continual improvement.

5.3 Policy

Top management shall establish a business continuity policy that

a) is appropriate to the purpose of the organization,

b) provides a framework for setting business continuity objectives,

c) includes a commitment to satisfy applicable requirements,

d) includes a commitment to continual improvement of the BCMS.

The BCMS policy shall

— be available as documented information,

— be communicated within the organization,

— be available to interested parties, as appropriate,

— be reviewed for continuing suitability at defined intervals and when significant changes occur

The organization shall retain documented information on the business continuity policy.

5.4 Organizational roles, responsibilities and authorities

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

Top management shall assign the responsibility and authority for

a) ensuring that the management system conforms to the requirements of this International Standard, and

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

Licensed to Leader & Reader Co,Ltd. / Ms. Sirirakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

6 Planning

6.1 Actions to address risks and opportunities

When planning for the BCMS, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to

— ensure the management system can achieve its intended outcome(s),

— prevent, or reduce, undesired effects,

— achieve continual improvement.

The organization shall plan

a) actions to address these risks and opportunities,

b) how to

   1) integrate and implement the actions into its BCMS processes (see 8.1),

   2) evaluate the effectiveness of these actions (see 9.1).

6.2 Business continuity objectives and plans to achieve them

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

The business continuity objectives shall

a) be consistent with the business continuity policy,

b) take account of the minimum level of products and services that is acceptable to the organization to achieve its objectives,

c) be measurable,

d) take into account applicable requirements, and

e) be monitored and updated as appropriate.

The organization shall retain documented information on the business continuity objectives.

To achieve its business continuity objectives, the organization shall determine

— who will be responsible,

— what will be done,

— what resources will be required,

— when it will be completed, and

— how the results will be evaluated.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the BCMS.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

7.2 Competence

The organization shall

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

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

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

d) retain appropriate documented information as evidence of competence.

NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the reassignment of current employed persons; or the hiring or contracting of competent persons.

7.3 Awareness

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

a) the business continuity policy,

b) their contribution to the effectiveness of the BCMS, including the benefits of improved business continuity management performance,

c) the implications of not conforming with the BCMS requirements, and

d) their own role during disruptive incidents.

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the BCMS including

a) on what it will communicate,

b) when to communicate,

c) with whom to communicate.

The organization shall establish, implement, and maintain procedure(s) for

— internal communication amongst interested parties and employees within the organization,

— external communication with customers, partner entities, local community, and other interested parties, including the media,

— receiving, documenting, and responding to communication from interested parties,

— adapting and integrating a national or regional threat advisory system, or equivalent, into planning and operational use, if appropriate,

— ensuring availability of the means of communication during a disruptive incident,

— facilitating structured communication with appropriate authorities and ensuring the interoperability of multiple responding organizations and personnel, where appropriate, and

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

NOTE Further requirements for communication in response to an incident are specified in 8.4.3.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

7.5 Documented information

7.5.1 General

The organization's BCMS shall include

— documented information required by this International Standard, and

— documented information determined by the organization as being necessary for the effectiveness of the BCMS.

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

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

— the complexity of processes and their interactions, and

— the competence of persons.

7.5.2 Creating and updating

When creating and updating documented information, the organization shall ensure appropriate

a) identification and description (e.g. a title, date, author or reference number),

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic), and review and approval for suitability and adequacy.

7.5.3 Control of documented information

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

a) it is available and suitable for use, where and when it is needed,

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable

— distribution, access, retrieval and use,

— storage and preservation, including preservation of legibility,

— control of changes (e.g. version control),

— retention and disposition,

— retrieval and use,

— preservation of legibility (i.e. clear enough to read), and

— prevention of the unintended use of obsolete information.

Documented information of external origin determined by the organization to be necessary for the planning and operation of the BCMS shall be identified, as appropriate, and controlled.

When establishing control of documented information, the organization shall ensure that there is adequate protection for the documented information (e.g. protection against compromise, unauthorized modification or deletion).

NOTE Access implies a decision regarding the permission to view the documented information, or the permission and authority to view and change the documented information, etc.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

8 Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in 6.1, by

a) establishing criteria for the processes,

b) implementing control of the processes in accordance with the criteria, and

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

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are controlled.

8.2 Business impact analysis and risk assessment

8.2.1 General

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

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

b) takes into account legal and other requirements to which the organization subscribes,

c) includes systematic analysis, prioritization of risk treatments, and their related costs,

d) defines the required output from the business impact analysis and risk assessment, and

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

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

8.2.2 Business impact analysis

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

The business impact analysis shall include the following:

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

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

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

d) identifying dependencies and supporting resources for these activities, including suppliers, outsource partners and other relevant interested parties.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

8.2.3 Risk assessment

The organization shall establish, implement, and maintain a formal documented risk assessment process that systematically identifies, analyses, and evaluates the risk of disruptive incidents to the organization.

NOTE This process could be made in accordance with ISO 31000.

The organization shall

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

b) systematically analyse risk,

c) evaluate which disruption related risks require treatment, and

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

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

8.3 Business continuity strategy

8.3.1 Determination and selection

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

The organization shall determine an appropriate business continuity strategy for

a) protecting prioritized activities,

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

c) mitigating, responding to and managing impacts.

The determination of strategy shall include approving prioritized time frames for the resumption of activities.

The organization shall conduct evaluations of the business continuity capabilities of suppliers.

8.3.2 Establishing resource requirements

The organization shall determine the resource requirements to implement the selected strategies. The types of resources considered shall include but not be limited to

a) people,

b) information and data,

c) buildings, work environment and associated utilities,

d) facilities, equipment and consumables,

e) information and communication technology (ICT) systems,

f) transportation,

g) finance, and

h) partners and suppliers.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

8.3.3 Protection and mitigation

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

a) reduce the likelihood of disruption,

b) shorten the period of disruption, and

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

The organization shall choose and implement appropriate risk treatments in accordance with its risk appetite.

8.4 Establish and implement business continuity procedures

8.4.1 General

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

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

The procedures shall

a) establish an appropriate internal and external communications protocol,

b) be specific regarding the immediate steps that are to be taken during a disruption,

c) be flexible to respond to unanticipated threats and changing internal and external conditions,

d) focus on the impact of events that could potentially disrupt operations,

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

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

8.4.2 Incident response structure

The organization shall establish, document, and implement procedures and a management structure to respond to a disruptive incident using personnel with the necessary responsibility, authority and competence to manage an incident.

The response structure shall

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

b) assess the nature and extent of a disruptive incident and its potential impact,

c) activate an appropriate business continuity response,

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

e) have resources available to support the processes and procedures to manage a disruptive incident in order to minimize impact, and

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

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

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

8.4.3 Warning and communication

The organization shall establish, implement and maintain procedures for

a) detecting an incident,

b) regular monitoring of an incident,

c) internal communication within the organization and receiving, documenting and responding to communication from interested parties,

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

e) assuring availability of the means of communication during a disruptive incident,

f) facilitating structured communication with emergency responders,

g) recording of vital information about the incident, actions taken and decisions made, and the following shall also be considered and implemented where applicable:

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

— assuring the interoperability of multiple responding organizations and personnel;

— operation of a communications facility.

The communication and warning procedures shall be regularly exercised.

8.4.4 Business continuity plans

The organization shall establish documented procedures for responding to a disruptive incident and how it will continue or recover its activities within a predetermined timeframe. Such procedures shall address the requirements of those who will use them.

The business continuity plans shall collectively contain

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

b) a process for activating the response,

c) details to manage the immediate consequences of a disruptive incident giving due regard to

   1) the welfare of individuals,

   2) strategic, tactical and operational options for responding to the disruption, and

   3) prevention of further loss or unavailability of prioritized activities;

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

e) how the organization will continue or recover its prioritized activities within predetermined timeframes,

f) details of the organization's media response following an incident, including

   1) a communications strategy,

   2) preferred interface with the media,

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

   4) appropriate spokespeople;

g) a process for standing down once the incident is over.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

Each plan shall define

— purpose and scope,

— objectives,

— 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.

8.4.5 Recovery

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

8.5 Exercising and testing

The organization shall exercise and test its business continuity procedures to ensure that they are consistent with its business continuity objectives.

The organization shall conduct exercises and tests that

a) are consistent with the scope and objectives of the BCMS,

b) are based on appropriate scenarios that are well planned with clearly defined aims and objectives,

c) taken together over time validate the whole of its business continuity arrangements, involving relevant interested parties,

d) minimize the risk of disruption of operations,

e) produce formalized post-exercise reports that contain outcomes, recommendations and actions to implement improvements,

f) are reviewed within the context of promoting continual improvement, and

g) are conducted at planned intervals and when there are significant changes within the organization or to the environment in which it operates.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.1.1 General

The organization shall determine

a) what needs to be monitored and measured,

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results,

c) when the monitoring and measuring shall be performed, and

Licensed to Leader & Reader Co.,Ltd. / Ms. Critsakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

d) when the results from monitoring and measurement shall be analysed and evaluated.

The organization shall retain appropriate documented information as evidence of the results.

The organization shall evaluate the BCMS performance and the effectiveness of the BCMS.

Additionally, the organization shall

— take action when necessary to address adverse trends or results before a nonconformity occurs, and

— retain relevant documented information as evidence of the results.

The procedures for monitoring performance shall provide for

— the setting of performance metrics appropriate to the needs of the organization,

— monitoring the extent to which the organization's business continuity policy, objectives and targets are met,

— performance of the processes, procedures and functions that protect its prioritized activities,

— monitoring compliance with this International Standard and the business continuity objectives,

— monitoring historical evidence of deficient BCMS' performance, and

— recording data and results of monitoring and measurement to facilitate subsequent corrective actions.

NOTE Deficient performance could include non-conformity, near misses, false alarms, and actual incidents.

9.1.2 Evaluation of business continuity procedures

a) The organization shall conduct evaluations of its business continuity procedures and capabilities in order to ensure their continuing suitability, adequacy and effectiveness;

b) These evaluations shall be undertaken through periodic reviews, exercising, testing, post-incident reporting and performance evaluations. Significant changes arising shall be reflected in the procedure(s) in a timely manner;

c) The organization shall periodically evaluate compliance with applicable legal and regulatory requirements, industry best practices, and conformance with its own business continuity policy and objectives; and

d) The organization shall conduct evaluations at planned intervals and when significant changes occur.

When a disruptive incident occurs and results in the activation of its business continuity procedures, the organization shall undertake a post-incident review and record the results.

9.2 Internal audit

The organization shall conduct internal audits at planned intervals to provide information on whether the business continuity management system

a) conforms to

   1) the organization's own requirements for its BCMS,

   2) the requirements of this International Standard, and

b) is effectively implemented and maintained.

The organization shall

— plan, establish, implement and maintain (an) audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits,

— define the audit criteria and scope for each audit,

Licensed to Leader & Binder Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

— select auditors and conduct audits to ensure objectivity and the impartiality of the audit process,

— ensure that the results of the audits are reported to relevant management, and

— retain documented information as evidence of the implementation of the audit programme and the audit results.

The audit programme, including any schedule, shall be based on the results of risk assessments of the organization's activities, and the results of previous audits. The audit procedures shall cover the scope, frequency, methodologies and competencies, as well as the responsibilities and requirements for conducting audits and reporting results.

The management responsible for the area being audited shall ensure that any necessary corrections and corrective actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results.

9.3 Management review

Top management shall review the organization's BCMS, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of

a) the status of actions from previous management reviews,

b) changes in external and internal issues that are relevant to the business continuity management system,

c) information on the business continuity performance, including trends in

   1) nonconformities and corrective actions,

   2) monitoring and measurement evaluation results, and

   3) audit results,

d) opportunities for continual improvement.

Management reviews shall consider the performance of the organization, including

— follow-up actions from previous management reviews,

— the need for changes to the BCMS, including the policy and objectives,

— opportunities for improvement,

— results of BCMS audits and reviews, including those of key suppliers and partners where appropriate,

— techniques, products or procedures, which could be used in the organization to improve the BCMS' performance and effectiveness,

— status of corrective actions,

— results of exercising and testing,

— risks or issues not adequately addressed in any previous risk assessment,

— any changes that could affect the BCMS, whether internal or external to the scope of the BCMS,

— adequacy of policy,

— recommendations for improvement,

— lessons learned and actions arising from disruptive incidents, and

— emerging good practice and guidance.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

The outputs of the management review shall include decisions related to continual improvement opportunities and the possible need for changes to the BCMS, and include the following:

a) variations to the scope of the BCMS;

b) improvement of the effectiveness of the BCMS;

c) update of the risk assessment, business impact analysis, business continuity plans and related procedures;

d) modification of procedures and controls to respond to internal or external events that may impact on the BCMS, including changes to

   1) business and operational requirements,

   2) risk reduction and security requirements,

   3) operational conditions and processes,

   4) legal and regulatory requirements,

   5) contractual obligations,

   6) levels of risk and/or criteria for accepting risks,

   7) resource needs,

   8) funding and budget requirements; and

e) how the effectiveness of controls are measured.

The organization shall retain documented information as evidence of the results of management reviews.

The organization shall

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

— take appropriate action relating to those results.

10 Improvement

10.1 Nonconformity and corrective action

When nonconformity occurs, the organization shall

a) identify the nonconformity,

b) react to the nonconformity, and, as applicable,

   1) take action to control and correct it, and

   2) deal with the consequences.

c) evaluate the need for action to eliminate the causes of the nonconformity, in order that it does not recur or occur elsewhere, by

   1) reviewing the nonconformity,

   2) determining the causes of the nonconformity, and

   3) determining if similar nonconformities exist, or could potentially occur,

   4) evaluating the need for corrective action to ensure that nonconformities do not recur or occur elsewhere,

   5) determining and implementing corrective action needed,

Licensed to Leonardo Paradise Cruzeiro Mrs. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

 © ISO 2012 – All rights reserved

6) reviewing the effectiveness of any corrective action taken and

7) making changes to the BCMS, if necessary.

d) implement any action needed,

e) review the effectiveness of any corrective action taken,

f) make changes to the business continuity management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The organization shall retain documented information as evidence of

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

— the results of any corrective action.

10.2 Continual improvement

The organization shall continually improve the suitability, adequacy or effectiveness of the BCMS.

NOTE The organization can use the processes of the BCMS such as leadership, planning and performance evaluation, to achieve improvement.

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

Bibliography

[1] ISO 9001, *Quality management systems — Requirements*

[2] ISO 14001, *Environmental management systems — Requirements with guidance for use*

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

[4] ISO/IEC 20000-1, *Information Technology — Service Management*

[5] ISO 22300, *Societal security — Terminology*

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

[7] ISO/IEC 24762, *Information technology — Security techniques — Guidelines for Information and communications technology disaster recovery services*

[8] ISO/IEC 27001, *Information Security Management Systems*

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

[10] ISO 31000, *Risk Management — Principles and Guidelines*

[11] ISO/IEC 31010, *Risk management — Risk assessment techniques*

[12] ISO/IEC Guide 73, *Risk management — Vocabulary*

[13] BS 25999-1, *Business continuity management — Code of practice*, British Standards Institution (BSI)

[14] BS 25999-2, *Business continuity management — Specification*, British Standards Institution (BSI)

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

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

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

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

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

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

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

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

ICS 03.100.01

Price based on 24 pages

Licensed to Leader & Reader Co;Ltd. / Ms. Sritrakool
ISO Store order #: 10-1348612/Downloaded: 2013-09-03
Single user licence only, copying and networking prohibited

© ISO 2012 – All rights reserved