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)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

ISO 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.

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.

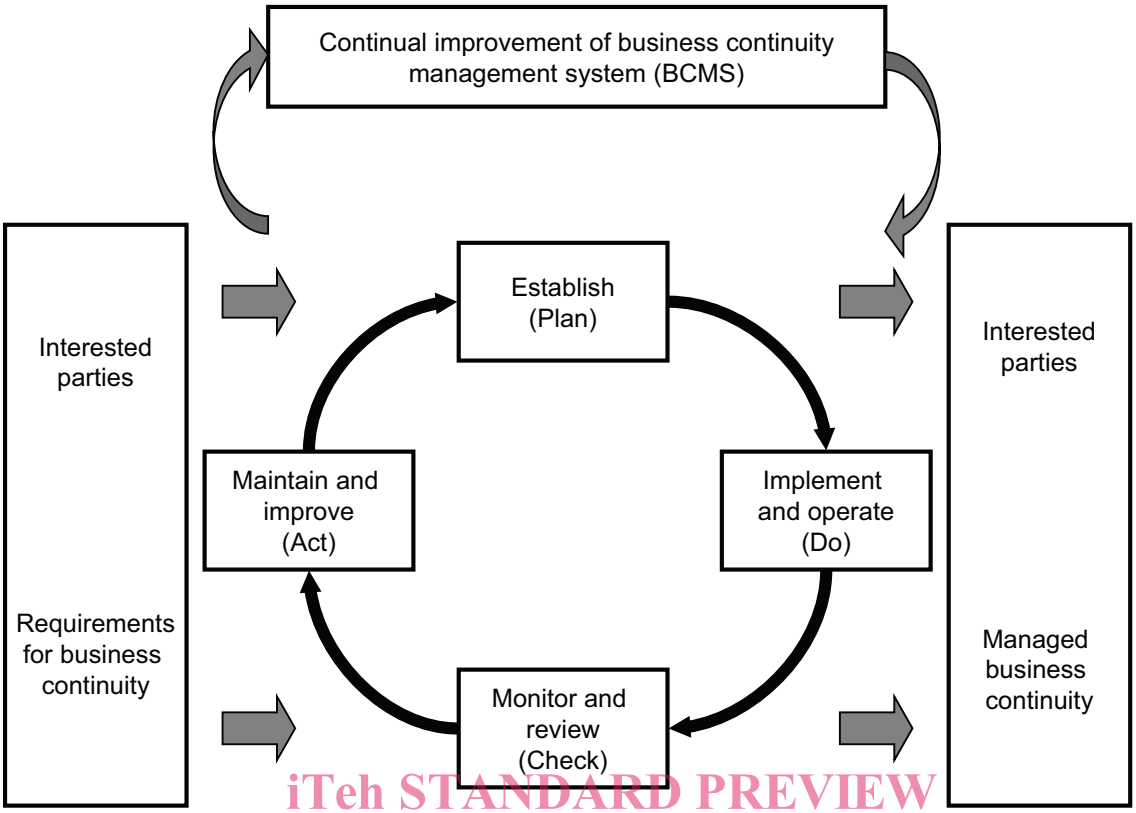

Figure 1 — PDCA model applied to BCMS processes

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.

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.

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.

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]

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]

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.