INTERNATIONAL STANDARD

ISO 22313

First edition
2012-12-15

Societal security — Business continuity management systems — Guidance

Sécurité sociétale — Systèmes de management de la continuité d'activité — Lignes directrices

Reference number
ISO 22313:2012(E)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

For the purposes of research, users are encouraged to share their views on ISO 22313:2012 and their priorities for changes to future editions of the document. Click on the link below to take part in the online survey:

http://www.surveymonkey.com/s/22313

Introduction

General

This International Standard provides guidance, where appropriate, on the requirements specified in ISO 22301:2012 and provides recommendations ('should') and permissions ('may') in relation to them. It is not the intention of this International Standard to provide general guidance on all aspects of business continuity.

This International Standard includes the same headings as ISO 22301 but does not repeat the requirements for business continuity management systems and its related terms and definitions. Organizations wishing to be informed of these must therefore refer to ISO 22301 and ISO 22300.

To provide further clarification and explanation of key points, this International Standard includes a number of figures. All such figures are for illustrative purposes only and the related text in the body of this International Standard takes precedence.

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

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

— implementing and operating controls and measures for managing an organization's overall capability to manage disruptive incidents;

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

— continual improvement based on objective measurement.

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

a) a policy;

b) people with defined responsibilities;

c) management processes relating to:

   1) policy;

   2) planning;

   3) implementation and operation;

   4) performance assessment;

   5) management review; and

   6) improvement.

d) a set of documentation providing auditable evidence; and

e) any BCMS processes relevant to the organization.

Business continuity is generally specific to an organization, however, its implementation can have far reaching implications on the wider community and other third parties. An organization is likely to have external organizations that it depends upon and there will be others that depend on it. Effective business continuity therefore contributes to a more resilient society.

The Plan-Do-Check-Act cycle

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

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

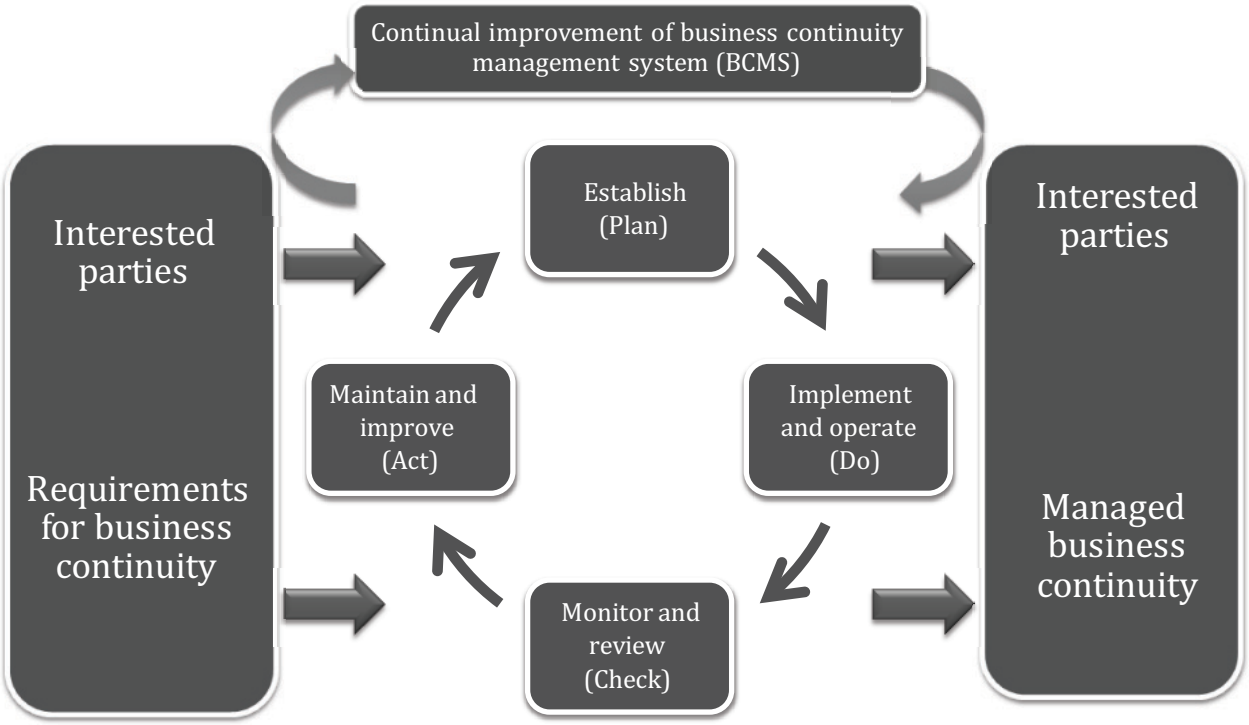

Figure 1 — PDCA model applied to BCMS processes

Table 1 — Explanation of PDCA model

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

Components of PDCA in this International Standard

There is a direct relationship between the content of Figure 1 and the clauses of this International Standard:

Table 2 — Relationship between PDCA model and Clauses 4 to 10

PDCA component	Clause addressing PDCA component
Plan (Establish)	**Clause 4 (Context of the organization)** sets out what the organization has to do in order to make sure that the BCMS meets its requirements, taking into account all relevant external and internal factors, including:
	— The needs and expectations of interested parties.
	— Its legal and regulatory obligations.
	— The required scope of the BCMS.
	Clause 5 (Leadership) sets out the key role of management in terms of demonstrating commitment, defining policy and establishing roles, responsibilities and authorities.
	Clause 6 (Planning) describes the actions required to establish strategic objectives and guiding principles for the BCMS as a whole. These set the context for the business impact analysis and risk assessment (8.2) and business continuity strategy (8.3).
	Clause 7 (Support) identifies the key elements that need to be in place to support the BCMS, namely: resources, competence, awareness, communication and documented information.
Do (Implement and operate)	**Clause 8 (Operation)** identifies the elements of business continuity management (BCM) that are needed to achieve business continuity.
Check (Monitor and review)	**Clause 9 (Performance evaluation)** provides the basis for improvement of the BCMS through measurement and evaluation of its performance.
Act (Maintain and improve)	**Clause 10 (Improvement)** covers the corrective action needed to address nonconformity identified through performance evaluation.

Business continuity

Business continuity is the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident. Business continuity management (BCM) is the process of achieving business continuity and is about preparing an organization to deal with disruptive incidents that might otherwise prevent it from achieving its objectives.

Placing BCM within the framework and disciplines of a management system creates a business continuity management system (BCMS) that enables BCM to be controlled, evaluated and continually improved.

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

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

BCM involves:

a) being clear on the organization's key products and services and the activities that deliver them;

b) knowing the priorities for resuming activities and the resources they require;

c) having a clear understanding of the threats to these activities, including their dependencies, and knowing the impacts of not resuming them;

d) having tried and trusted arrangements in place to resume these activities following a disruptive incident; and