
**Societal security — Business continuity
management systems — Guidance**

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



This document is a preview generated by EVIS



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

Contents

	Page
Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Context of the organization	1
4.1 Understanding of the organization and its context.....	1
4.2 Understanding the needs and expectations of interested parties.....	2
4.3 Determining the scope of the management system.....	4
4.4 Business continuity management system.....	4
5 Leadership	4
5.1 Leadership and commitment.....	4
5.2 Management commitment.....	5
5.3 Policy.....	5
5.4 Organizational roles, responsibilities and authorities.....	6
6 Planning	7
6.1 Actions to address risks and opportunities.....	7
6.2 Business continuity objectives and plans to achieve them.....	7
7 Support	7
7.1 Resources.....	7
7.2 Competence.....	8
7.3 Awareness.....	10
7.4 Communication.....	11
7.5 Documented information.....	12
8 Operation	14
8.1 Operational planning and control.....	14
8.2 Business impact analysis and risk assessment.....	17
8.3 Business continuity strategy.....	21
8.4 Establish and implement business continuity procedures.....	28
8.5 Exercising and testing.....	38
9 Performance evaluation	40
9.1 Monitoring, measurement, analysis and evaluation.....	40
9.2 Internal audit.....	42
9.3 Management review.....	43
10 Improvement	44
10.1 Nonconformity and corrective action.....	44
10.2 Continual improvement.....	45
Bibliography	46

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.

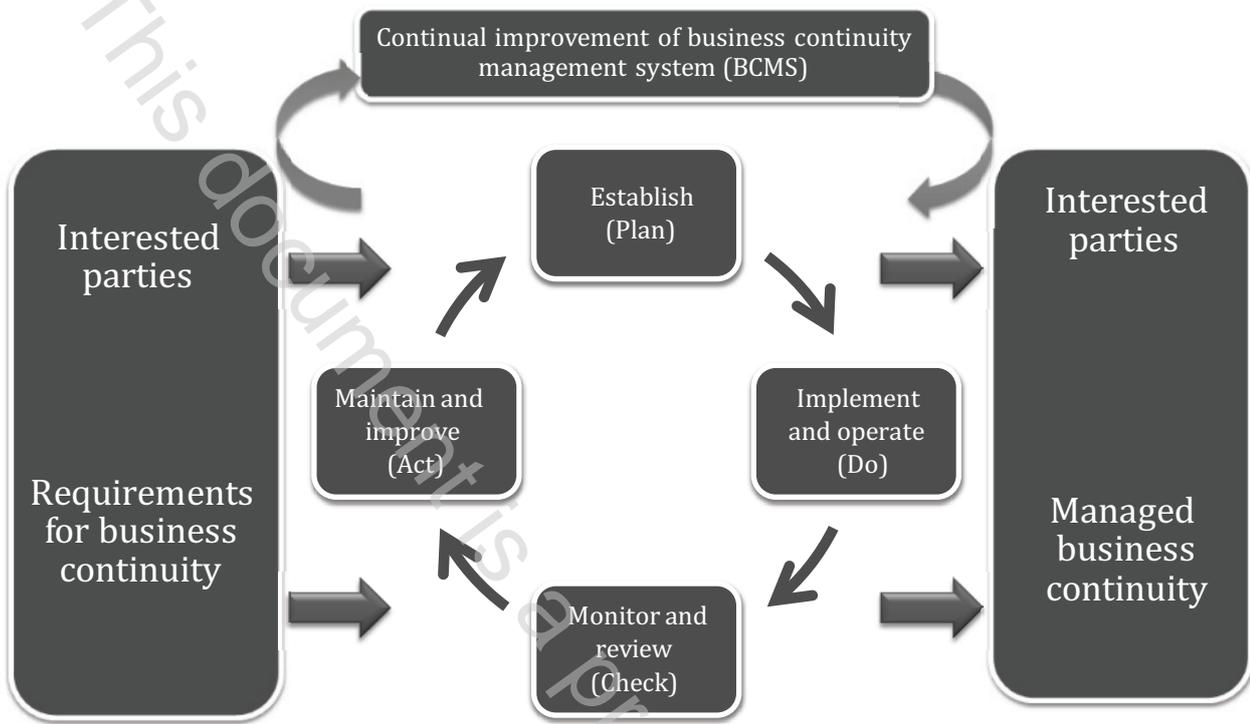


Figure 1 — PDCA model applied to BCMS processes

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.
Do (Implement and operate)	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.
Check (Monitor and review)	Clause 8 (Operation) identifies the elements of business continuity management (BCM) that are needed to achieve business continuity.
Act (Maintain and improve)	Clause 9 (Performance evaluation) provides the basis for improvement of the BCMS through measurement and evaluation of its performance.
	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

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

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

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

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

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

Mitigating impacts through effective business continuity – sudden disruption

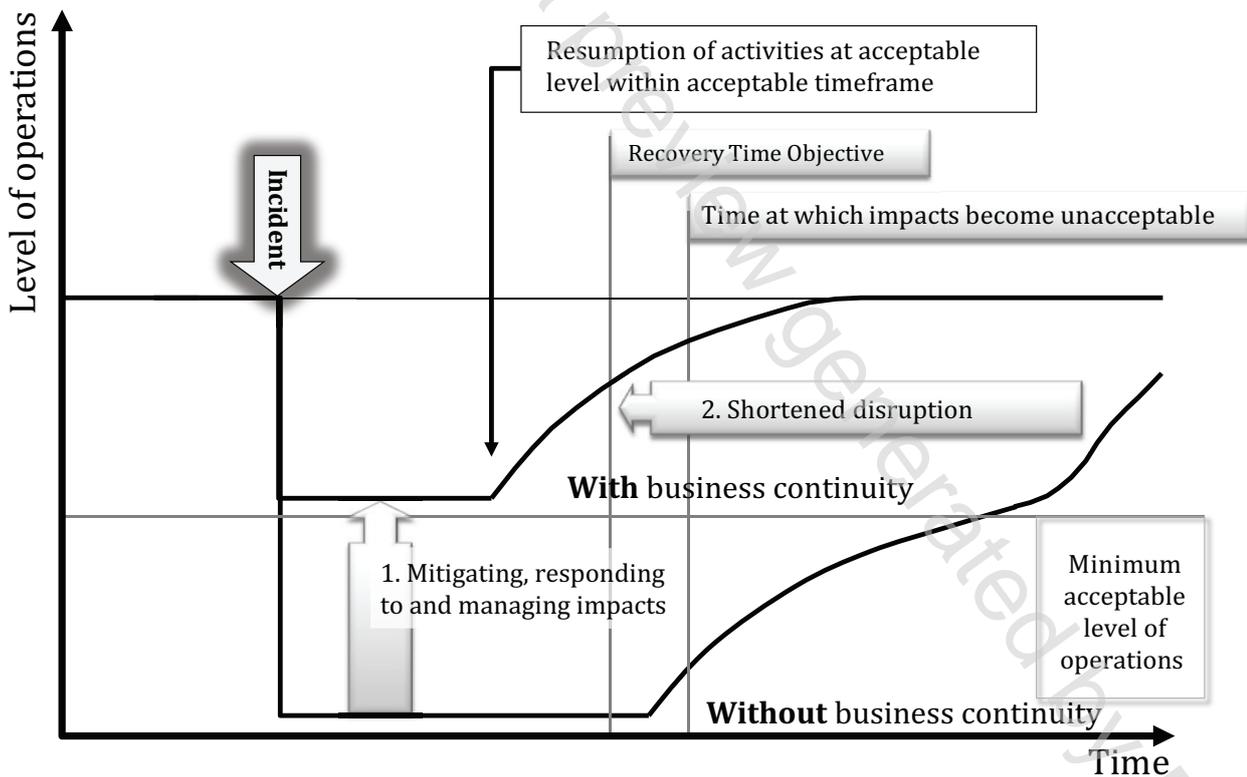


Figure 2 — Illustration of business continuity being effective for sudden disruption

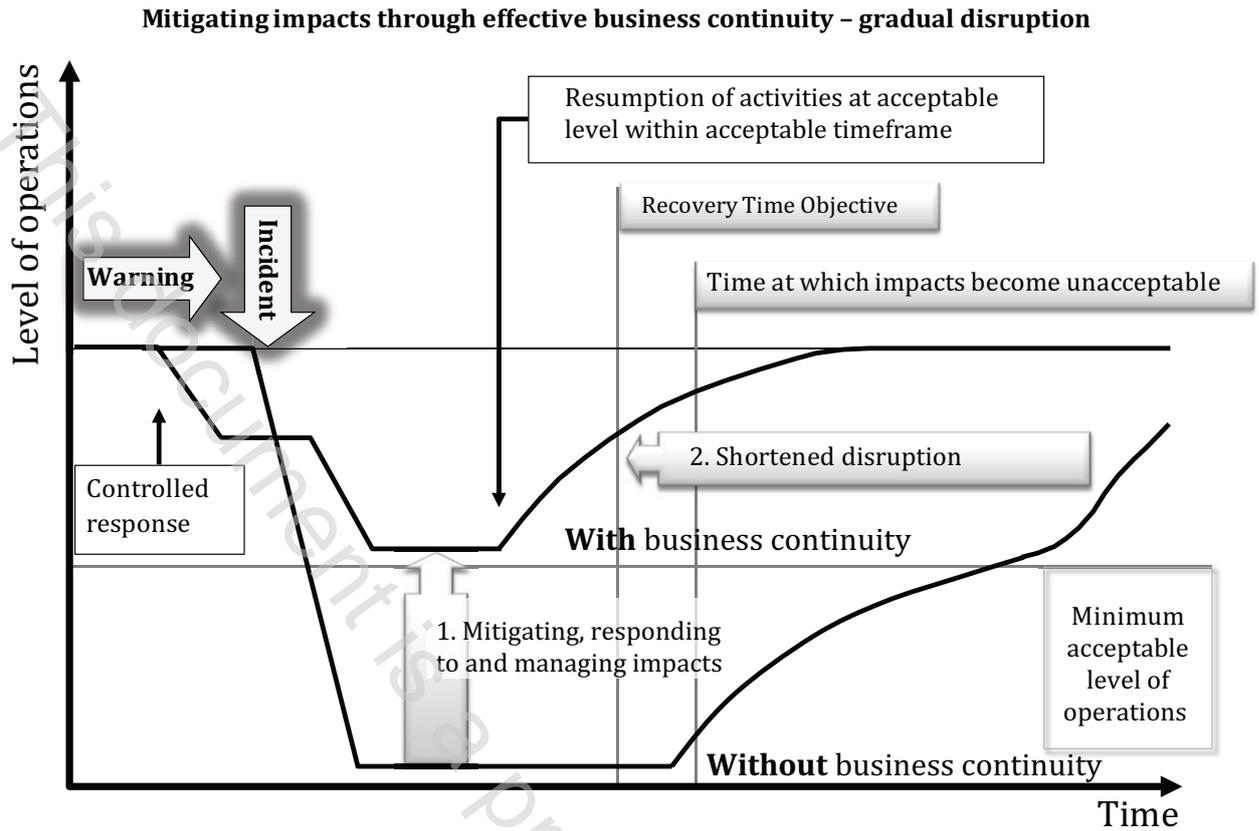


Figure 3 — Illustration of business continuity being effective for gradual disruption (e.g. approaching pandemic)

Societal security — Business continuity management systems — Guidance

1 Scope

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

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

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

- a) establish, implement, maintain and improve a BCMS;
- b) ensure conformance with the organization's business continuity policy; or
- c) make a self-determination and self-declaration of compliance with this International Standard.

This International Standard cannot be used to assess an organization's ability to meet its own business continuity needs, nor any customer, legal or regulatory needs. Organizations wishing to do so can use the ISO 22301 requirements to demonstrate conformance to others or seek certification of its BCMS by an accredited third party certification body.

2 Normative references

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

ISO 22300, *Societal security — Terminology*

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

3 Terms and definitions

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

4 Context of the organization

4.1 Understanding of the organization and its context

This section is about understanding the context of the organization in relation to setting up and managing the BCMS. The setting up and management of BCM is covered in 8.1.