

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)



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
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

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.