



DRAFT INTERNATIONAL STANDARD ISO/DIS 22301

ISO/TC 223

Secretariat: SIS

Voting begins on
2010-11-26

Voting terminates on
2011-04-26

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

Societal security — Preparedness and continuity management systems — Requirements

Sécurité sociétale — État de préparation et systèmes de gestion de la continuité — Exigences

ICS 03.100.01

In accordance with the provisions of Council Resolution 15/1993 this document is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 15/1993, ce document est distribué en version anglaise seulement.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

© International Organization for Standardization, 2010

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Copyright notice

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to 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

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Contents

Page

Foreword	v
Introduction.....	vi
0.1 General	vi
0.2 The Plan-Do-Check-Act (PDCA) cycle.....	vi
1 Scope	1
2 Normative references.....	1
3 Terms and definitions	1
4 General requirements	6
4.1 Understanding of the organization and its context	6
4.2 Needs and requirements.....	6
4.3 Management system and scope	6
5 Leadership	6
5.1 General	6
5.2 Management commitment	7
5.3 Policy	7
5.4 Organizational roles, responsibilities and authorities	7
6 Planning	8
6.1 Objectives and plans to achieve them	8
6.2 Action to address issues and concerns	8
7 Support.....	9
7.1 Resources	9
7.2 Competence	9
7.3 Awareness.....	9
7.4 Communication	9
7.4.1 External communication.....	9
7.4.2 Internal communication	9
7.5 Documented information	9
7.5.1 General	9
7.5.2 Create and update	10
7.5.3 Control of documented Information	10
8 Operation.....	10
8.1 General	10
8.2 Operational planning and control.....	11
8.3 Preparation.....	11
8.4 Planning	12
8.4.1 Management commitment	12
8.4.2 Policy development.....	12
8.4.3 Business impact analysis and risk assessment	13
8.4.4 Business continuity options	14
8.5 Performing	15
8.5.1 Developing and implementing a business continuity response	15
8.5.2 Response structure.....	15
8.5.3 Warning and communication	16
8.5.4 Response	16
8.5.5 Business continuity plans.....	17
8.5.6 Response procedure requirements.....	17
8.5.7 Response procedure content.....	17
8.5.8 Recovery	18

8.5.9	Communication and consultation	18
8.6	Checking	19
8.6.1	Exercising and testing	19
8.6.2	Monitoring performance	19
8.7	Reviewing	19
8.7.1	Management review	19
8.7.2	Evaluation of continuity procedures	20
9	Performance evaluation	21
9.1	Monitoring and measurement	21
9.2	Internal audit	21
9.3	Management review	22
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.

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

Introduction

General

This International Standard specifies requirements for setting up and managing an effective Business Continuity Management System (BCMS).

This emphasizes the importance of:

- a) understanding continuity and preparedness needs and the necessity for establishing business continuity management policy and objectives;
- b) implementing and operating controls and measures for managing an organization's overall continuity risks;
- c) monitoring and reviewing the performance and effectiveness of the BCMS; and
- d) continual improvement based on objective measurement.

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

- e) a policy;
- f) people with defined responsibilities;
- g) management processes relating to:
 - 1) policy;
 - 2) planning;
 - 3) implementation and operation;
 - 4) performance assessment;
 - 5) management review; and
 - 6) improvement;
- h) a set of documentation providing auditable evidence; and
- i) any business continuity management processes relevant to the organization.

The Plan-Do-Check-Act (PDCA) cycle

The standard applies the "Plan-Do-Check-Act" (PDCA) cycle to planning, establishing, implementing, operating, monitoring, reviewing, exercising, 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 9001:2008 (Quality Management Systems), ISO 14001:2004 (Environmental Management Systems), ISO/IEC 27001:2005 (Information Security Management Systems) and ISO/IEC 20000-1:2005 (Information

Technology - Service Management), thereby supporting consistent and integrated implementation and operation with related management systems (see Annex A).

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



Figure 1 — PDCA cycle applied to BCMS processes

Societal security — Preparedness and continuity management systems — Requirements

1 Scope

This International Standard for business continuity specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to prepare for, respond to and recover from disruption.

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 stakeholders' requirements. These needs are shaped by regulatory, organizational and industry requirements, the products and services, the processes employed, the size and structure of the organization, and the requirements of its stakeholders.

This International Standard is applicable to all types and sizes of organizations that wish to:

- a) establish, implement, maintain and improve a BCMS;
- b) assure conformance with stated BCMS policy;
- c) demonstrate conformance to others;
- d) seek certification/registration of its BCMS system by an accredited third party certification body; or
- e) make a self-determination and self-declaration of conformance 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 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 (including any amendments) applies.

ISO/IEC Guide 73: 2009, *Risk management — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC Guide 73:2009 and the following apply.

3.1
audit
process for obtaining evidence and assessing it objectively to determine the extent to which specified requirements are fulfilled

3.2
business continuity management
management process which provides a framework for building capability that safeguards the objectives of the organization including its obligations.

3.3
business impact analysis
process of analysing business functions and the effect at the business disruption might have upon them

3.4
competence
demonstrated ability to apply knowledge and skills to achieve intended results

3.5
conformity
fulfilment of a requirement

3.6
continual improvement
recurring activity to enhance performance

3.7
correction
action to eliminate a detected nonconformity

3.8
corrective action
action to eliminate the cause of a nonconformity or other undesirable situation and to prevent recurrence

3.9
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"

3.10
effectiveness
extent to which planned activities are realized and planned results achieved

3.11
efficiency
relationship between the result achieved and the resources used

3.12
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".