

# INTERNATIONAL STANDARD

# ISO 22301

Second edition  
2019-10

---

---

## Security and resilience — Business continuity management systems — Requirements

*Sécurité et résilience — Systèmes de management de la continuité  
d'activité — Exigences*





**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Fax: +41 22 749 09 47  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

	Page
Foreword .....	v
Introduction .....	vi
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Context of the organization</b> .....	<b>7</b>
4.1 Understanding the organization and its context .....	7
4.2 Understanding the needs and expectations of interested parties .....	7
4.2.1 General .....	7
4.2.2 Legal and regulatory requirements .....	7
4.3 Determining the scope of the business continuity management system .....	7
4.3.1 General .....	7
4.3.2 Scope of the business continuity management system .....	8
4.4 Business continuity management system .....	8
<b>5 Leadership</b> .....	<b>8</b>
5.1 Leadership and commitment .....	8
5.2 Policy .....	8
5.2.1 Establishing the business continuity policy .....	8
5.2.2 Communicating the business continuity policy .....	9
5.3 Roles, responsibilities and authorities .....	9
<b>6 Planning</b> .....	<b>9</b>
6.1 Actions to address risks and opportunities .....	9
6.1.1 Determining risks and opportunities .....	9
6.1.2 Addressing risks and opportunities .....	9
6.2 Business continuity objectives and planning to achieve them .....	9
6.2.1 Establishing business continuity objectives .....	9
6.2.2 Determining business continuity objectives .....	10
6.3 Planning changes to the business continuity management system .....	10
<b>7 Support</b> .....	<b>10</b>
7.1 Resources .....	10
7.2 Competence .....	10
7.3 Awareness .....	11
7.4 Communication .....	11
7.5 Documented information .....	11
7.5.1 General .....	11
7.5.2 Creating and updating .....	11
7.5.3 Control of documented information .....	12
<b>8 Operation</b> .....	<b>12</b>
8.1 Operational planning and control .....	12
8.2 Business impact analysis and risk assessment .....	12
8.2.1 General .....	12
8.2.2 Business impact analysis .....	13
8.2.3 Risk assessment .....	13
8.3 Business continuity strategies and solutions .....	13
8.3.1 General .....	13
8.3.2 Identification of strategies and solutions .....	13
8.3.3 Selection of strategies and solutions .....	14
8.3.4 Resource requirements .....	14
8.3.5 Implementation of solutions .....	14
8.4 Business continuity plans and procedures .....	14
8.4.1 General .....	14

8.4.2	Response structure.....	15
8.4.3	Warning and communication .....	15
8.4.4	Business continuity plans .....	16
8.4.5	Recovery.....	17
8.5	Exercise programme .....	17
8.6	Evaluation of business continuity documentation and capabilities .....	17
<b>9</b>	<b>Performance evaluation .....</b>	<b>17</b>
9.1	Monitoring, measurement, analysis and evaluation.....	17
9.2	Internal audit.....	18
9.2.1	General.....	18
9.2.2	Audit programme(s).....	18
9.3	Management review.....	18
9.3.1	General.....	18
9.3.2	Management review input .....	18
9.3.3	Management review outputs .....	19
<b>10</b>	<b>Improvement.....</b>	<b>19</b>
10.1	Nonconformity and corrective action.....	19
10.2	Continual improvement.....	20
	<b>Bibliography .....</b>	<b>21</b>

## 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see [www.iso.org/directives](http://www.iso.org/directives)).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see [www.iso.org/patents](http://www.iso.org/patents)).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html).

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

This second edition cancels and replaces the first edition (ISO 22301:2012), which has been technically revised. The main changes compared with the previous edition are as follows:

- ISO's requirements for management system standards, which have evolved since 2012, have been applied;
- requirements have been clarified, with no new requirements added;
- discipline-specific business continuity requirements are now almost entirely within [Clause 8](#);
- [Clause 8](#) has been re-structured to provide a clearer understanding of the key requirements;
- a number of discipline-specific business continuity terms have been modified to improve clarity and to reflect current thinking.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at [www.iso.org/members.html](http://www.iso.org/members.html).

## Introduction

### 0.1 General

This document specifies the structure and requirements for implementing and maintaining a business continuity management system (BCMS) that develops business continuity appropriate to the amount and type of impact that the organization may or may not accept following a disruption.

The outcomes of maintaining a BCMS are shaped by the organization's legal, regulatory, organizational and industry requirements, products and services provided, processes employed, size and structure of the organization, and the requirements of its interested parties.

A BCMS emphasizes the importance of:

- understanding the organization's needs and the necessity for establishing business continuity policies and objectives;
- operating and maintaining processes, capabilities and response structures for ensuring the organization will survive disruptions;
- monitoring and reviewing the performance and effectiveness of the BCMS;
- continual improvement based on qualitative and quantitative measures.

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

- a) a policy;
- b) competent people with defined responsibilities;
- c) management processes relating to:
  - 1) policy;
  - 2) planning;
  - 3) implementation and operation;
  - 4) performance assessment;
  - 5) management review;
  - 6) continual improvement;
- d) documented information supporting operational control and enabling performance evaluation.

### 0.2 Benefits of a business continuity management system

The purpose of a BCMS is to prepare for, provide and maintain controls and capabilities for managing an organization's overall ability to continue to operate during disruptions. In achieving this, the organization is:

- a) from a business perspective:
  - 1) supporting its strategic objectives;
  - 2) creating a competitive advantage;
  - 3) protecting and enhancing its reputation and credibility;