

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*



Reference number
ISO 22301:2019(E)

© ISO 2019

ISO 22301:2019(E)



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
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Context of the organization	7
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
5 Leadership	8
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
6 Planning	9
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
7 Support	10
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
8 Operation	12
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

ISO 22301:2019(E)

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
9	Performance evaluation	17
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
10	Improvement	19
10.1	Nonconformity and corrective action	19
10.2	Continual improvement	20
	Bibliography	21

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).

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).

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.

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.

ISO 22301:2019(E)

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;

- 4) contributing to organizational resilience;
- b) from a financial perspective:
 - 1) reducing legal and financial exposure;
 - 2) reducing direct and indirect costs of disruptions;
- c) from the perspective of interested parties:
 - 1) protecting life, property and the environment;
 - 2) considering the expectations of interested parties;
 - 3) providing confidence in the organization's ability to succeed;
- d) from an internal processes perspective:
 - 1) improving its capability to remain effective during disruptions;
 - 2) demonstrating proactive control of risks effectively and efficiently;
 - 3) addressing operational vulnerabilities.

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

This document applies the Plan (establish), Do (implement and operate), Check (monitor and review) and Act (maintain and improve) (PDCA) cycle to implement, maintain and continually improve the effectiveness of an organization's BCMS.

This ensures a degree of consistency with other management systems standards, such as ISO 9001, ISO 14001, ISO/IEC 20000-1, ISO/IEC 27001 and ISO 28000, thereby supporting consistent and integrated implementation and operation with related management systems.

In accordance with the PDCA cycle, [Clauses 4](#) to [10](#) cover the following components.

- [Clause 4](#) introduces the requirements necessary to establish the context of the BCMS applicable to the organization, as well as needs, requirements and scope.
- [Clause 5](#) summarizes the requirements specific to top management's role in the BCMS, and how leadership articulates its expectations to the organization via a policy statement.
- [Clause 6](#) describes the requirements for establishing strategic objectives and guiding principles for the BCMS as a whole.
- [Clause 7](#) supports BCMS operations related to establishing competence and communication on a recurring/as-needed basis with interested parties, while documenting, controlling, maintaining and retaining required documented information.
- [Clause 8](#) defines business continuity needs, determines how to address them and develops procedures to manage the organization during a disruption.
- [Clause 9](#) summarizes the requirements necessary to measure business continuity performance, BCMS conformity with this document, and to conduct management review.
- [Clause 10](#) identifies and acts on BCMS nonconformity and continual improvement through corrective action.

0.5 Contents of this document

This document conforms to ISO's requirements for management system standards. These requirements include a high level structure, identical core text and common terms with core definitions, designed to benefit users implementing multiple ISO management system standards.

ISO 22301:2019(E)

This document does not include requirements specific to other management systems, though its elements can be aligned or integrated with those of other management systems.

This document contains requirements that can be used by an organization to implement a BCMS and to assess conformity. An organization that wishes to demonstrate conformity to this document can do so by:

- making a self-determination and self-declaration; or
- seeking confirmation of its conformity by parties having an interest in the organization, such as customers; or
- seeking confirmation of its self-declaration by a party external to the organization; or
- seeking certification/registration of its BCMS by an external organization.

[Clauses 1](#) to [3](#) in this document set out the scope, normative references and terms and definitions that apply to the use of this document. [Clauses 4](#) to [10](#) contain the requirements to be used to assess conformity to this document.

In this document, the following verbal forms are used:

- a) “shall” indicates a requirement;
- b) “should” indicates a recommendation;
- c) “may” indicates a permission;
- d) “can” indicates a possibility or a capability.

Information marked as “NOTE” is for guidance in understanding or clarifying the associated requirement. “Notes to entry” used in [Clause 3](#) provide additional information that supplements the terminological data and can contain provisions relating to the use of a term.

Security and resilience — Business continuity management systems — Requirements

1 Scope

This document specifies requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise.

The requirements specified in this document 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.

This document is applicable to all types and sizes of organizations that:

- a) implement, maintain and improve a BCMS;
- b) seek to ensure conformity with stated business continuity policy;
- c) need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption;
- d) seek to enhance their resilience through the effective application of the BCMS.

This document can be used to assess an organization's ability to meet its own business continuity needs and obligations.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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, *Security and resilience — Vocabulary*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

NOTE The terms and definitions given below supersede those given in ISO 22300:2018.

3.1 activity

set of one or more tasks with a defined output

[SOURCE: ISO 22300:2018, 3.1, modified — The definition has been replaced and the example has been deleted.]

ISO 22301:2019(E)

3.2 audit

systematic, independent and documented *process* (3.26) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: An internal audit is conducted by the *organization* (3.21) itself, or by an external party on its behalf.

Note 3 to entry: “Audit evidence” and “audit criteria” are defined in ISO 19011.

Note 4 to entry: The fundamental elements of an audit include the determination of the *conformity* (3.7) of an object according to a procedure carried out by personnel not being responsible for the object audited.

Note 5 to entry: An internal audit can be for management review and other internal purposes and can form the basis for an organization’s declaration of conformity. Independence can be demonstrated by the freedom from responsibility for the *activity* (3.1) being audited. External audits include second- and third-party audits. Second-party audits are conducted by parties having an interest in the organization, such as customers, or by other persons on their behalf. Third-party audits are conducted by external, independent auditing organizations, such as those providing certification/registration of conformity or government agencies.

Note 6 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards. The original definition has been modified by adding Notes 4 and 5 to entry.

3.3 business continuity

capability of an *organization* (3.21) to continue the delivery of *products and services* (3.27) within acceptable time frames at predefined capacity during a *disruption* (3.10)

[SOURCE: ISO 22300:2018, 3.24, modified — The definition has been replaced.]

3.4 business continuity plan

documented information (3.11) that guides an *organization* (3.21) to respond to a *disruption* (3.10) and resume, recover and restore the delivery of *products and services* (3.27) consistent with its *business continuity* (3.3) *objectives* (3.20)

[SOURCE: ISO 22300:2018, 3.27, modified — The definition has been replaced and Note 1 to entry has been deleted.]

3.5 business impact analysis

process (3.26) of analysing the *impact* (3.13) over time of a *disruption* (3.10) on the *organization* (3.21)

Note 1 to entry: The outcome is a statement and justification of *business continuity* (3.3) *requirements* (3.28).

[SOURCE: ISO 22300:2018, 3.29, modified — The definition has been replaced and Note 1 to entry has been added.]

3.6 competence

ability to apply knowledge and skills to achieve intended results

Note 1 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.7 conformity

fulfilment of a *requirement* (3.28)

Note 1 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.8
continual improvement

recurring *activity* (3.1) to enhance *performance* (3.23)

Note 1 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.9
corrective action

action to eliminate the cause(s) of a *nonconformity* (3.19) and to prevent recurrence

Note 1 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.10
disruption

incident (3.14), whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of *products and services* (3.27) according to an *organization's* (3.21) *objectives* (3.20)

[SOURCE: ISO 22300:2018, 3.70, modified — The definition has been replaced.]

3.11
documented information

information required to be controlled and maintained by an *organization* (3.21) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media, and from any source.

Note 2 to entry: Documented information can refer to:

- the *management system* (3.16), including related *processes* (3.26);
- information created in order for the organization to operate (documentation);
- evidence of results achieved (records).

Note 3 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.12
effectiveness

extent to which planned *activities* (3.1) are realized and planned results achieved

Note 1 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.13
impact

outcome of a *disruption* (3.10) affecting *objectives* (3.20)

[SOURCE: ISO 22300:2018, 3.107, modified — The definition has been replaced.]

3.14
incident

event that can be, or could lead to, a *disruption* (3.10), loss, emergency or crisis

[SOURCE: ISO 22300:2018, 3.111, modified — The definition has been replaced.]