



BSI Standards Publication

Security and resilience — Business continuity management systems — Requirements

National foreword

This British Standard is the UK implementation of EN ISO 22301:2019+A1:2024. It is identical to ISO 22301:2019, incorporating amendment 1:2024. It supersedes BS EN ISO 22301:2019, which is withdrawn.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to ISO text carry the number of the ISO amendment. For example, text altered by ISO amendment 1 is indicated by A1 A1.

The UK participation in its preparation was entrusted to Technical Committee CAR/1, Continuity and Resilience.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 30393 3

ICS 03.100.01; 03.100.70

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2019.

Amendments/corrigenda issued since publication

Date	Text affected
30 September 2024	Implementation of ISO amendment 1:2024 with CEN endorsement A1:2024

English Version

Security and resilience - Business continuity management systems - Requirements (ISO 22301:2019)

Sécurité et résilience - Systèmes de management de la continuité d'activité - Exigences (ISO 22301:2019)

Sicherheit und Resilienz - Business Continuity Management System - Anforderungen (ISO 22301:2019)

This European Standard was approved by CEN on 14 October 2019.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

This document (EN ISO 22301:2019) has been prepared by Technical Committee ISO/TC 292 "Security and resilience" in collaboration with Technical Committee CEN/TC 391 "Societal and Citizen Security" the secretariat of which is held by AFNOR.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by May 2020, and conflicting national standards shall be withdrawn at the latest by May 2020.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO 22301:2014.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 22301:2019 has been approved by CEN as EN ISO 22301:2019 without any modification.

European foreword to amendment A1

The text of ISO 22301:2019/Amd 1:2024 has been prepared by Technical Committee ISO/TC 292 "Security and resilience" of the International Organization for Standardization (ISO) and has been taken over as EN ISO 22301:2019/A1:2024 by Technical Committee CEN/TC 391 "Societal and Citizen Security" the secretariat of which is held by AFNOR.

This Amendment to the European Standard EN ISO 22301:2019 shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by March 2025, and conflicting national standards shall be withdrawn at the latest by March 2025.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN website.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO 22301:2019/Amd 1:2024 has been approved by CEN as EN ISO 22301:2019/A1:2024 without any modification.

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

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.

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.

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.