

## DIN EN ISO 22313



ICS 03.100.01; 03.100.70

Supersedes  
DIN EN ISO 22313:2016-05

**Security and resilience –  
Business continuity management systems –  
Guidance on the use of ISO 22301 (ISO 22313:2020);  
English version EN ISO 22313:2020,  
English translation of DIN EN ISO 22313:2020-10**

Sicherheit und Resilienz –  
Business Continuity Management System –  
Anleitung zur Verwendung von ISO 22301 (ISO 22313:2020);  
Englische Fassung EN ISO 22313:2020,  
Englische Übersetzung von DIN EN ISO 22313:2020-10

Sécurité et résilience –  
Systèmes de management de la continuité d'activité –  
Lignes directrices sur l'utilisation de l'ISO 22301 (ISO 22313:2020);  
Version anglaise EN ISO 22313:2020,  
Traduction anglaise de DIN EN ISO 22313:2020-10

Document comprises 71 pages

Translation by DIN-Sprachendienst.

In case of doubt, the German-language original shall be considered authoritative.

*A comma is used as the decimal marker.*

## **National foreword**

This document (EN ISO 22313:2020) has been prepared by Technical Committee ISO/TC 292 “Security and resilience” in collaboration with Technical Committee CEN/TC 391 “Societal and citizen security” (Secretariat: AFNOR, France).

The responsible German body involved in its preparation was *DIN-Normenausschuss Organisationsprozesse* (DIN Standards Committee for Organizational Processes), Joint Working Committee NA 175-00-05 GA “Security and Business Continuity”.

The DIN documents corresponding to the international documents referred to in this document are as follows:

ISO 19011	DIN EN ISO 19011
ISO 22300	DIN EN ISO 22300
ISO 22301	DIN EN ISO 22301
ISO 31000	DIN ISO 31000
ISO/IEC 27002	DIN EN ISO/IEC 27002

## **Amendments**

This standard differs from DIN EN ISO 22313:2016-05 as follows:

- a) the content and structure of the document have been aligned with the latest edition of ISO 22301;
- b) additional explanations to individual terms and definitions have been added;
- c) the contents of 8.4 have been removed to include them in ISO/TS 22332 in the future;
- d) the standard has been editorially revised.

## **Previous editions**

DIN EN ISO 22313: 2016-05

**National Annex NA**  
(informative)

**Bibliography**

DIN EN ISO 19011, *Guidelines for auditing management systems*

DIN EN ISO 22300, *Security and resilience — Vocabulary*

DIN EN ISO 22301, *Security and resilience — Business continuity management system — Requirements*

DIN EN ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

DIN ISO 31000, *Risk management — Principles and guidelines*

— This page is intentionally blank —

English Version

Security and resilience -  
Business continuity management systems -  
Guidance on the use of ISO 22301  
(ISO 22313:2020)

Sécurité et résilience -  
Systèmes de management de la continuité d'activité -  
Lignes directrices sur l'utilisation de l'ISO 22301  
(ISO 22313:2020)

Sicherheit und Resilienz -  
Business Continuity Management System -  
Anleitung zur Verwendung von ISO 22301  
(ISO 22313:2020)

This European Standard was approved by CEN on 18 February 2020.

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

# Contents

Page

<b>European foreword</b>	<b>4</b>
<b>Foreword</b>	<b>5</b>
<b>Introduction</b>	<b>6</b>
<b>1 Scope</b>	<b>13</b>
<b>2 Normative references</b>	<b>13</b>
<b>3 Terms and definitions</b>	<b>13</b>
<b>4 Context of the organization</b>	<b>14</b>
4.1 Understanding the organization and its context	14
4.2 Understanding the needs and expectations of interested parties	15
4.2.1 General	15
4.2.2 Legal and regulatory requirements	15
4.3 Determining the scope of the business continuity management system	16
4.3.1 General	16
4.3.2 Scope of the business continuity management system	16
4.3.3 Exclusions to scope	16
4.4 Business continuity management system	17
<b>5 Leadership</b>	<b>17</b>
5.1 Leadership and commitment	17
5.1.1 General	17
5.1.2 Top management	17
5.1.3 Other managerial roles	18
5.2 Policy	18
5.2.1 Establishing the business continuity policy	18
5.2.2 Communicating the business continuity policy	19
5.3 Roles, responsibilities and authorities	19
<b>6 Planning</b>	<b>21</b>
6.1 Actions to address risks and opportunities	21
6.1.1 Determining risks and opportunities	21
6.1.2 Addressing risks and opportunities	21
6.2 Business continuity objectives and planning to achieve them	22
6.2.1 Establishing business continuity objectives	22
6.2.2 Determining business continuity objectives	22
6.3 Planning changes to the business continuity management system	22
<b>7 Support</b>	<b>23</b>
7.1 Resources	23
7.1.1 General	23
7.1.2 BCMS resources	23
7.2 Competence	23
7.3 Awareness	25
7.4 Communication	26
7.5 Documented information	27
7.5.1 General	27
7.5.2 Creating and updating	28
7.5.3 Control of documented information	28

<b>8</b>	<b>Operation</b>	<b>29</b>
8.1	Operational planning and control	29
8.1.1	General	29
8.1.2	Business continuity management	30
8.1.3	Maintaining business continuity	31
8.2	Business impact analysis and risk assessment	32
8.2.1	General	32
8.2.2	Business impact analysis	32
8.2.3	Risk assessment	35
8.3	Business continuity strategies and solutions	37
8.3.1	General	37
8.3.2	Identification of strategies and solutions	37
8.3.3	Selection of strategies and solutions	40
8.3.4	Resource requirements	40
8.3.5	Implementation of solutions	46
8.4	Business continuity plans and procedures	47
8.4.1	General	47
8.4.2	Response structure	47
8.4.3	Warning and communication	48
8.4.4	Business continuity plans	50
8.4.5	Recovery	55
8.5	Exercise programme	56
8.5.1	General	56
8.5.2	Design of the exercise programme	56
8.5.3	Exercising business continuity plans	57
8.6	Evaluation of business continuity documentation and capabilities	60
8.6.1	General	60
8.6.2	Measuring effectiveness	61
8.6.3	Outcomes	61
<b>9</b>	<b>Performance evaluation</b>	<b>62</b>
9.1	Monitoring, measurement, analysis and evaluation	62
9.1.1	General	62
9.1.2	Retention of evidence	62
9.1.3	Performance evaluation	62
9.2	Internal audit	63
9.2.1	General	63
9.2.2	Audit programme(s)	63
9.3	Management review	63
9.3.1	General	63
9.3.2	Management review input	63
9.3.3	Management review outputs	63
<b>10</b>	<b>Improvement</b>	<b>64</b>
10.1	Nonconformity and corrective action	64
10.1.1	General	64
10.1.2	Occurrence of nonconformity	65
10.1.3	Retention of documented information	65
10.2	Continual improvement	65
	<b>Bibliography</b>	<b>67</b>

## **European foreword**

This document (EN ISO 22313:2020) 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 August 2020, and conflicting national standards shall be withdrawn at the latest by August 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 22313:2014.

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 22313:2020 has been approved by CEN as EN ISO 22313:2020 without any modification.

## 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 22313:2012), which has been technically revised. The main changes compared with the previous edition are as follows:

- structural and content alterations have been made to align this document with the latest edition of ISO 22301;
- additional guidance has been added to explain key concepts and terms;
- content has been removed from [8.4](#) that will be included in ISO/TS 22332 (under development).

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).