



SLOVENSKI STANDARD SIST EN ISO 22313:2020

01-maj-2020

Nadomešča:
SIST EN ISO 22313:2015

Varnost in vzdržljivost - Sistem vodenja neprekinjenosti poslovanja - Navodilo za uporabo standarda ISO 22301 (ISO 22313:2020)

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

Sicherheit und Resilienz - Business Continuity Management Systems - Anleitung zur Verwendung von 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)

Ta slovenski standard je istoveten z: EN ISO 22313:2020

ICS:

03.100.01	Organizacija in vodenje podjetja na splošno	Company organization and management in general
03.100.70	Sistemi vodenja	Management systems

SIST EN ISO 22313:2020

en,fr,de

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO 22313:2020

<https://standards.iteh.ai/catalog/standards/sist/2ed5285d-8183-4dec-a09e-07592dc09081/sist-en-iso-22313-2020>

EUROPEAN STANDARD

EN ISO 22313

NORME EUROPÉENNE

EUROPÄISCHE NORM

February 2020

ICS 03.100.01; 03.100.70

Supersedes EN ISO 22313:2014

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 Systems - 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.

iTeh STANDARD PREVIEW

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
European foreword.....	3

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO 22313:2020
<https://standards.iteh.ai/catalog/standards/sist/2ed5285d-8183-4dec-a09e-07592dc09081/sist-en-iso-22313-2020>

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.

iTeh STANDARD PREVIEW
Endorsement notice
(standards.iteh.ai)

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

<https://standards.iteh.ai/catalog/standards/sist/2ed5285d-8183-4dec-a09e-07592dc09081/sist-en-iso-22313-2020>

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO 22313:2020

<https://standards.iteh.ai/catalog/standards/sist/2ed5285d-8183-4dec-a09e-07592dc09081/sist-en-iso-22313-2020>

INTERNATIONAL
STANDARD

ISO
22313

Second edition
2020-02

**Security and resilience — Business
continuity management systems —
Guidance on the use of ISO 22301**

*Sécurité et résilience — Systèmes de management de la continuité
d'activité — Lignes directrices sur l'utilisation de l'ISO 22301*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN ISO 22313:2020](https://standards.iteh.ai/catalog/standards/sist/2ed5285d-8183-4dec-a09e-07592dc09081/sist-en-iso-22313-2020)

<https://standards.iteh.ai/catalog/standards/sist/2ed5285d-8183-4dec-a09e-07592dc09081/sist-en-iso-22313-2020>



Reference number
ISO 22313:2020(E)

© ISO 2020

iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN ISO 22313:2020

<https://standards.iteh.ai/catalog/standards/sist/2ed5285d-8183-4dec-a09e-07592dc09081/sist-en-iso-22313-2020>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2020

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	2
4.1 Understanding the organization and its context.....	2
4.2 Understanding the needs and expectations of interested parties.....	3
4.2.1 General.....	3
4.2.2 Legal and regulatory requirements.....	3
4.3 Determining the scope of the business continuity management system.....	4
4.3.1 General.....	4
4.3.2 Scope of the business continuity management system.....	4
4.3.3 Exclusions to scope.....	4
4.4 Business continuity management system.....	5
5 Leadership	5
5.1 Leadership and commitment.....	5
5.1.1 General.....	5
5.1.2 Top management.....	5
5.1.3 Other managerial roles.....	6
5.2 Policy.....	6
5.2.1 Establishing the business continuity policy.....	6
5.2.2 Communicating the business continuity policy.....	7
5.3 Roles, responsibilities and authorities.....	7
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.....	10
6.2.1 Establishing business continuity objectives.....	10
6.2.2 Determining business continuity objectives.....	10
6.3 Planning changes to the business continuity management system.....	10
7 Support	11
7.1 Resources.....	11
7.1.1 General.....	11
7.1.2 BCMS resources.....	11
7.2 Competence.....	11
7.3 Awareness.....	13
7.4 Communication.....	14
7.5 Documented information.....	15
7.5.1 General.....	15
7.5.2 Creating and updating.....	16
7.5.3 Control of documented information.....	16
8 Operation	17
8.1 Operational planning and control.....	17
8.1.1 General.....	17
8.1.2 Business continuity management.....	18
8.1.3 Maintaining business continuity.....	19
8.2 Business impact analysis and risk assessment.....	20
8.2.1 General.....	20
8.2.2 Business impact analysis.....	20

ISO 22313:2020(E)

8.2.3	Risk assessment.....	23
8.3	Business continuity strategies and solutions.....	25
8.3.1	General.....	25
8.3.2	Identification of strategies and solutions.....	25
8.3.3	Selection of strategies and solutions.....	28
8.3.4	Resource requirements.....	28
8.3.5	Implementation of solutions.....	34
8.4	Business continuity plans and procedures.....	35
8.4.1	General.....	35
8.4.2	Response structure.....	35
8.4.3	Warning and communication.....	36
8.4.4	Business continuity plans.....	38
8.4.5	Recovery.....	43
8.5	Exercise programme.....	44
8.5.1	General.....	44
8.5.2	Design of the exercise programme.....	44
8.5.3	Exercising business continuity plans.....	45
8.6	Evaluation of business continuity documentation and capabilities.....	48
8.6.1	General.....	48
8.6.2	Measuring effectiveness.....	49
8.6.3	Outcomes.....	49
9	Performance evaluation.....	50
9.1	Monitoring, measurement, analysis and evaluation.....	50
9.1.1	General.....	50
9.1.2	Retention of evidence.....	50
9.1.3	Performance evaluation.....	50
9.2	Internal audit.....	51
9.2.1	General.....	51
9.2.2	Audit programme(s).....	51
9.3	Management review.....	51
9.3.1	General.....	51
9.3.2	Management review input.....	51
9.3.3	Management review outputs.....	52
10	Improvement.....	52
10.1	Nonconformity and corrective action.....	52
10.1.1	General.....	52
10.1.2	Occurrence of nonconformity.....	53
10.1.3	Retention of documented information.....	53
10.2	Continual improvement.....	53
	Bibliography.....	55

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 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.

ISO 22313:2020(E)

Introduction

0.1 General

This document provides guidance, where appropriate, on the requirements specified in ISO 22301. It is not the intention of this document to provide general guidance on all aspects of business continuity.

This document includes the same clause headings as ISO 22301 but does not restate the requirements and related terms and definitions.

The intention of the guidance is to explain and clarify the meaning and purpose of the requirements of ISO 22301 and assist in the resolution of any issues of interpretation. Other International Standards and Technical Specifications that provide additional guidance, and to which reference is made in this document, are ISO/TS 22317, ISO/TS 22318, ISO 22322, ISO/TS 22330, ISO/TS 22331 and ISO 22398. The scope of these documents can extend beyond the requirements of ISO 22301. Organizations should therefore always refer to ISO 22301 to verify the requirements to be met.

To provide further clarification and explanation of key points, this document includes several figures. The figures are for illustrative purposes only and the related text in the body of this document takes precedence.

A business continuity management system (BCMS) emphasizes the importance of:

- establishing business continuity policy and objectives that align with the organization's 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 measurement.

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.

Business continuity is generally specific to an organization. However, its implementation can have far reaching implications on the wider community and other third parties. An organization is likely to have external organizations that it depends upon and there will be others that depend on it. Effective business continuity therefore contributes to a more resilient society.

0.2 Benefits of a business continuity management system

A BCMS increases the organization's level of preparedness to continue to operate during disruptions. It also results in improved understanding of the organization's internal and external relationships, better communication with interested parties and the creation of a continual improvement environment. There are potentially many additional benefits to implementing a BCMS in accordance with the recommendations contained in this document and in accordance with the requirements of ISO 22301.

- Following the recommendations in [Clause 4](#) (“context of the organization”) involves the organization:
 - reviewing its strategic objectives to ensure that the BCMS supports them;
 - reconsidering the needs, expectations and requirements of interested parties;
 - being aware of applicable legal, regulatory and other obligations.
- [Clause 5](#) (“leadership”) involves the organization:
 - reconsidering management roles and responsibilities;
 - promoting a culture of continual improvement;
 - allocating responsibility for performance monitoring and reporting.
- [Clause 6](#) (“planning”) involves the organization:
 - re-examining its risks and opportunities and identifying actions to address and take advantage of them;
 - establishing effective change management.
- [Clause 7](#) (“support”) involves the organization:
 - establishing effective management of its BCMS resources, including competence management;
 - improving employee awareness of matters that are important to management;
 - having effective mechanisms for internal and external communications;
 - managing its documentation effectively.
- [Clause 8](#) (“operation”) results in the organization considering:
 - the unintended consequences of change;
 - business continuity priorities and requirements;
 - dependencies;
 - vulnerabilities from an impact perspective;
 - risks of disruption and identifying how best to address them;
 - alternative solutions for running the business with limited resources;
 - effective structures and procedures for dealing with disruptions;
 - responsibilities to the community and other interested parties.
- [Clause 9](#) (“performance evaluation”) involves the organization:
 - having effective mechanisms for monitoring, measuring and evaluating performance;

ISO 22313:2020(E)

- involving management in monitoring the performance and contributing to the effectiveness of the BCMS.
- [Clause 10](#) (“improvement”) involves the organization:
 - having procedures for monitoring performance and improving effectiveness;
 - benefitting from continual improvement of its management systems.

As a result, implementation of the BCMS can:

- a) protect life, assets and the environment;
- b) protect and enhance the organization’s reputation and credibility;
- c) contribute to the organization’s competitive advantage by enabling it to operate during disruptions;
- d) reduce costs arising from disruptions and improving the organization’s capability to remain effective during them;
- e) contribute to the organization’s overall organizational resilience;
- f) assist in making interested parties more confident in the organization’s success;
- g) reduce the organization’s legal and financial exposure;
- h) demonstrate the organization’s ability to manage risk and address operational vulnerabilities.

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

This document applies the Plan-Do-Check-Act (PDCA) cycle to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organization’s BCMS. An explanation of the PDCA cycle is given in [Table 1](#).

[Figure 1](#) illustrates how the BCMS takes interested parties’ requirements as inputs for business continuity management and, through the required actions and processes, produces business continuity outcomes (i.e. managed business continuity) that meet those requirements.

Table 1 — Explanation of PDCA cycle

Plan (Establish)	Establish business continuity policy, objectives, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organization’s overall policies and objectives.
Do (Implement and operate)	Implement and operate the business continuity policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the BCMS by taking corrective actions, based on the results of management review and re-appraising the scope of the BCMS and business continuity policy and objectives.

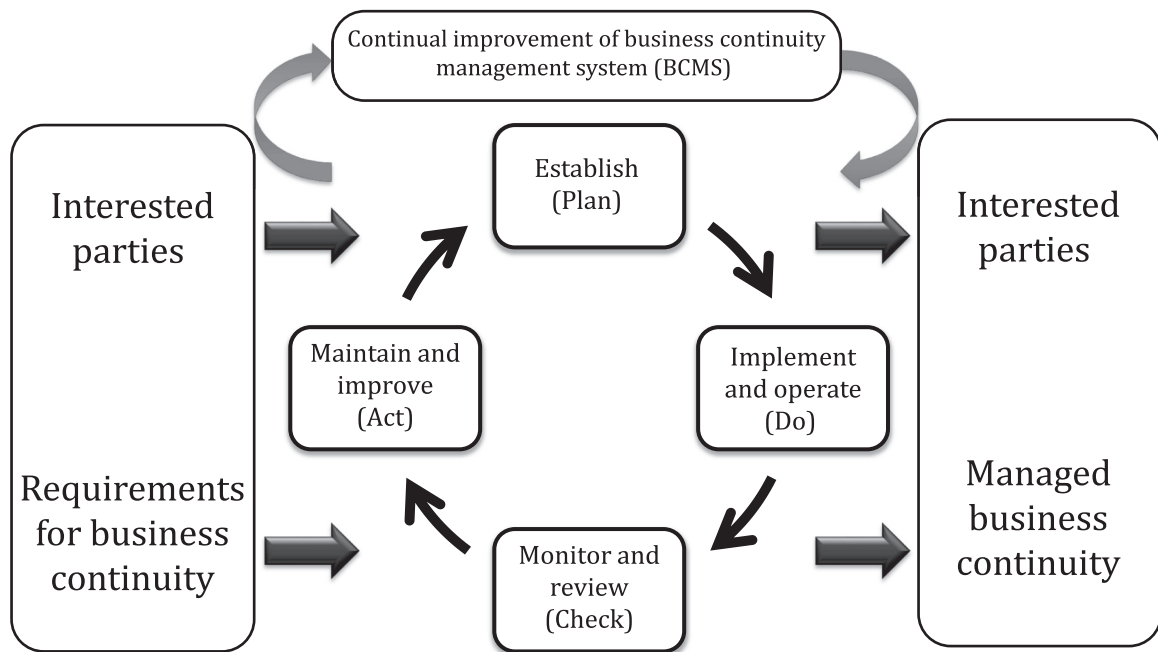


Figure 1 — PDCA cycle applied to BCMS processes

0.4 Components of PDCA in this document

Table 2 shows the direct relationship between the content of Figure 1 and the clauses of this document.

Table 2 — Relationship between the PDCA cycle and Clauses 4 to 10

PDCA component	Clause addressing PDCA component
Plan (Establish)	<p>Clause 4 (“context of the organization”) sets out what the organization should do in order to make sure that the BCMS meets its requirements, taking into account all relevant external and internal factors, including:</p> <ul style="list-style-type: none"> — the needs and expectations of interested parties; — its legal and regulatory obligations; — the required scope of the BCMS. <p>Clause 5 (“leadership”) sets out the role of management in terms of demonstrating commitment, defining policy and establishing roles, responsibilities and authorities.</p> <p>Clause 6 (“planning”) describes the actions for establishing strategic objectives and guiding principles for the implementation of the BCMS.</p> <p>Clause 7 (“support”) identifies the BCMS elements that should be in place, namely: resources, competence, awareness, communication and documented information.</p>
Do (Implement and operate)	Clause 8 (“operation”) identifies the processes for establishing and maintaining business continuity.
Check (Monitor and review)	Clause 9 (“performance evaluation”) provides the basis for improving the BCMS through measurement and evaluating its performance.
Act (Maintain and improve)	Clause 10 (“improvement”) covers the corrective action for addressing nonconformity identified through performance evaluation.

0.5 Contents of this document

It is not the intent of this document to imply uniformity in the structure of a BCMS but for an organization to design a BCMS that is appropriate to its needs and that meets the requirements of its interested parties, particularly customers and employees. These needs are shaped by legal, regulatory, organizational and industry requirements, the products and services, the processes employed, the