SLOVENSKI STANDARD
oSIST prEN ISO 22313:2019

01-junij-2019

Varnost in vzdržljivost - Sistem vodenja neprekinjenosti poslovanja - Navodilo (ISO/DIS 22313:2019)

Security and resilience - Business continuity management systems - Guidance (ISO/DIS 22313:2019)

Sicherheit und Resilienz - Business Continuity Management Systems - Leitlinie (ISO/DIS 22313:2019)

Sécurité et résilience - Systèmes de management de la continuité d'activité - Lignes directrices (ISO/DIS 22313:2019)

Ta slovenski standard je istoveten z: **prEN ISO 22313**

ICS:

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

oSIST prEN ISO 22313:2019 **en,fr,de**

DRAFT INTERNATIONAL STANDARD

ISO/DIS 22313

ISO/TC **292**

Secretariat: **SIS**

Voting begins on:
2019-04-17

Voting terminates on:
2019-07-10

Security and resilience — Business continuity management systems — Guidance

Sécurité et résilience — Systèmes de management de la continuité d'activité — Lignes directrices

ICS: 03.100.70; 03.100.01

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 22313:2019(E)

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

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 on 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 the following URL: www.iso.org/iso/foreword.html.

ISO 22313 was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

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 provides guidance, where appropriate, on the requirements specified in ISO 22301:201x Security and resilience – Business continuity management systems – Requirements and provides recommendations ('should') and permissions ('may') in relation to them. 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 ISO 22301 requirements and assist in the resolution of any issues of interpretation. There are other ISO publications that may provide additional guidance. Table 1 identifies other standards and technical specifications to which reference is made in this document. Technical specifications are not subject to the same level of scrutiny as requirements or guidance standards and do not have the same voting requirements. In addition, their scope may extend beyond the requirements of ISO 22301. Organizations should therefore always refer to ISO 22301 and this document to verify the requirements to be met.

Table 1 — Supporting documents

Number	Title
ISO/TS 22317	Societal security – Business continuity management systems – Guidelines for business impact analysis (BIA)
ISO/TS 22318	Societal security – Business continuity management systems – Guidelines for supply chain continuity
ISO 22322	Societal security - Emergency management – Guidelines for public warning
ISO/TS 22330	Security and resilience – Business continuity management systems – Guidelines for people aspects of business continuity
ISO/TS 22331	Security and resilience – Business continuity management systems – Guidelines for business continuity strategy
ISO 22398	Societal security – Guidelines for exercising

To provide further clarification and explanation of key points, this document includes several figures. All such 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:

— understanding the organization's needs and business objectives;

— involving people with suitable knowledge, skills and experience;

— establishing business continuity policy and objectives;

— improving the organization's capability to manage disruptions in a controlled manner;

— top management taking a leadership role;

— the performance and effectiveness of plans and procedures;

— continual improvement based on objective measurement.

Like any management system, a BCMS has:

a) a policy;

b) competent people with defined responsibilities;

c) management processes relating to:

- policy;
- planning;
- implementation and operation;
- performance assessment;
- management review;
- 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 BCMS

The benefits of a BCMS include a higher level of preparedness to handle disruption, improved understanding of the organization's internal and external relationships, better communications with interested parties and 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.

a) Implementing the recommendations in Clause 4 (Context of the organization) requires the organization to:

- review its strategic objectives to ensure that the BCMS supports them;
- reconsider the needs, expectations and requirements of interested parties;
- be aware of applicable legal, regulatory and other obligations;

b) Clause 5 (Leadership) requires the organization to:

- reconsider management roles and responsibilities;
- promote a culture of continual improvement;
- establish performance monitoring and reporting;

c) Clause 6 (Planning) requires the organization to:

- re-examine its risks and opportunities and identify actions to address and take advantage of them;
- establish effective change management;

d) Clause 7 (Support) requires the organization to:

- establish effective management of its BCMS resources, including competence management;
- improve employee awareness of matters that are important to management;
- have effective mechanisms for internal and external communications;
- manage its documentation effectively;

e) Clause 8 (Operation) requires the organization to:

- be aware of the unintended consequences of change;
- reconsider its dependency on external suppliers and its supply chain;
- reconsider vulnerabilities from an impact perspective;
- evaluate risks of disruption and identify how best to address them;
- come up with imaginative solutions for running the business with limited resources;
- implement effective structures and procedures for dealing with disruptions;
- be aware of its responsibilities to the community and other interested parties;

f) Clause 9 (Performance evaluation) requires the organization to:

- have effective mechanisms for monitoring, measuring and evaluating performance;
- involve management in the monitoring the performance and contributing to the effectiveness of the BCMS;

g) Clause 10 (Improvement) requires the organization to:

- have procedures for monitoring performance and improving effectiveness;
- benefit from continual improvement of its management systems.

As a result, implementation of the BCMS may:

a) protect life, property 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 disruptive incidents;

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 The 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.

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

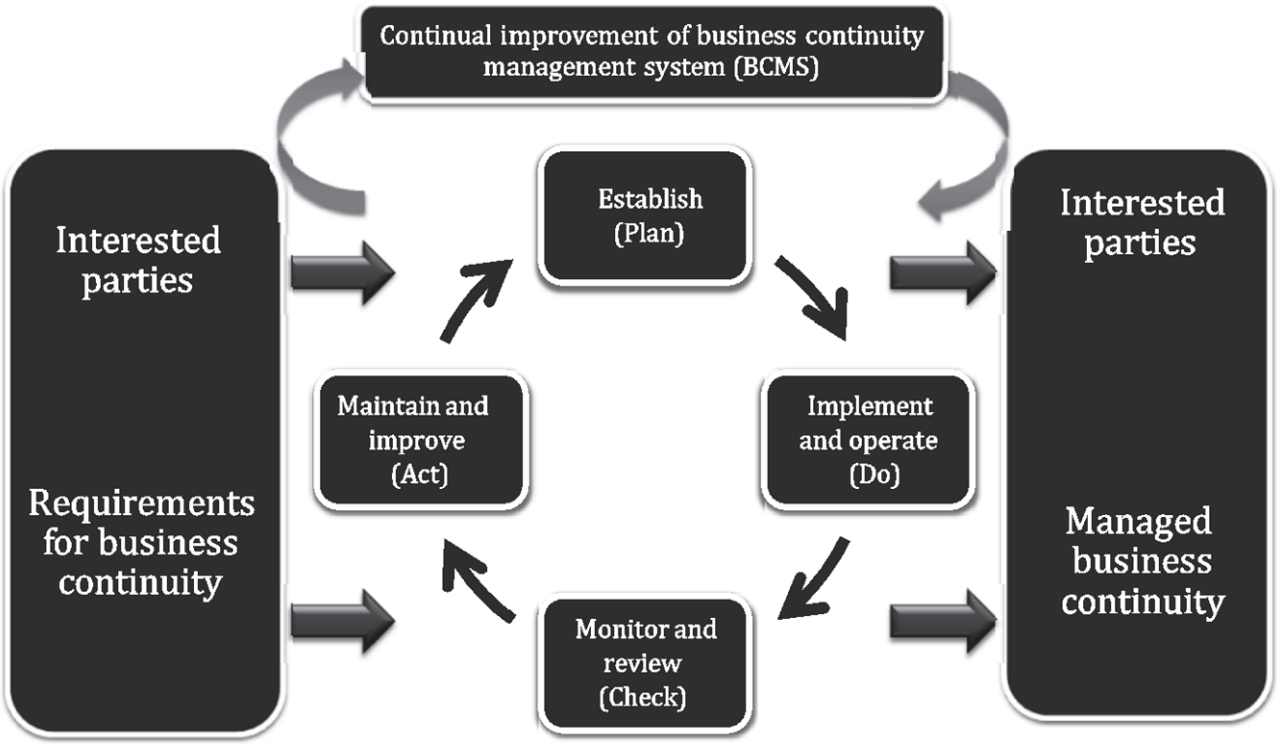

Figure 1 — PDCA model applied to BCMS processes

Table 2 — Explanation of PDCA model

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.

0.4 Components of PDCA in this document

There is a direct relationship between the content of Figure 1 and the clauses of this document:

Table 3 — Relationship between PDCA model and Clauses 4 to 10

PDCA component	Clause addressing PDCA component
Plan (Establish)	**Clause 4 (Context of the organization)** sets out what the organization has to do in order to make sure that the BCMS meets its requirements, taking into account all relevant external and internal factors, including: — the needs and expectations of interested parties; — its legal and regulatory obligations; — the required scope of the BCMS.
	Clause 5 (Leadership) sets out the role of management in terms of demonstrating commitment, defining policy and establishing roles, responsibilities and authorities.
	Clause 6 (Planning) describes the actions required to establish strategic objectives and guiding principles for the implementation of the BCMS.
	Clause 7 (Support) identifies the BCMS elements that need to be in place, namely: resources, competence, awareness, communication and documented information.
Do (Implement and operate)	**Clause 8 (Operation)** identifies the processes needed to establish business continuity.
Check (Monitor and review)	**Clause 9 (Performance evaluation)** provides the basis for improvement of the BCMS through measurement and evaluation of its performance.
Act (Maintain and improve)	**Clause 10 (Improvement)** covers the corrective action needed to address nonconformity identified through performance evaluation.

0.5 Contents of this document

Clauses 1 to 3 in this document set out the scope, normative references and terms and definitions which apply to the use of this document, while Clauses 4 to 10 contain guidance on the requirements to be used to assess conformity to ISO 22301.

In this document, the following verbal forms are used:

a) 'should' indicates a recommendation;

i) 'may' indicates a permission;

j) 'can' indicates a possibility or a capability.

0.6 Business continuity

Business continuity is the capability of the organization to continue delivery of products or services at acceptable predefined capacities following a disruption. Business continuity management (BCM) is the process of implementing and maintaining business continuity in order to prepare for, mitigate, and manage disruptions.

Establishing a BCMS enables the organization to control, evaluate and continually improve its business continuity.

In this document, the word business is used as an all-embracing term for the operations and services performed by an organization in pursuit of its objectives, goals or mission. As such it is equally applicable to large, medium and small organizations operating in industrial, commercial, public and not-for-profit sectors.

Disruptions have the potential to interrupt the organization's entire operations and its ability to deliver products and services. However, implementing a BCMS before a disruption occurs, rather than responding in an unplanned manner after the incident, will enable the organization to resume operations before unacceptable levels of impact arise.

BCM involves:

a) identifying the organization's products and services and the activities that deliver them;

b) analysing the impacts of not resuming the activities and the resources they depend on;

c) understanding the threats to the activities and their dependencies;

d) setting priorities, strategies and timeframes for resuming the delivery of products and services, activities and their dependencies;

e) having solutions and plans in place to resume the activities within the required timescales following a disruption;

f) making sure that these arrangements are routinely reviewed and updated so that they will be effective in all circumstances.

The organization's approach to BCM and system of documentation should be appropriate to its context (e.g. operating environment, complexity, needs and resources).

Business continuity can be effective in dealing with both sudden disruptions (e.g. explosions) and gradual ones (e.g. pandemics).

Activities can be disrupted by a wide variety of incidents, many of which are difficult to predict or analyse. By focusing on the impact of disruption rather than the cause, business continuity enables an organization to identify activities that are essential to it being able to meet its obligations. Through business continuity, an organization can recognize what needs to be done to protect its resources (e.g. people, premises, technology and information), supply chain, interested parties and reputation, before a disruption occurs. With that recognition, the organization can put in place a response structure, so that it can be confident of managing the impacts of a disruption.

The following diagrams (Figure 2 and Figure 3) are intended to illustrate conceptually how business continuity can be effective in mitigating impacts in certain situations. No particular timescales are implied by the relative distance between the stages depicted in either diagram.

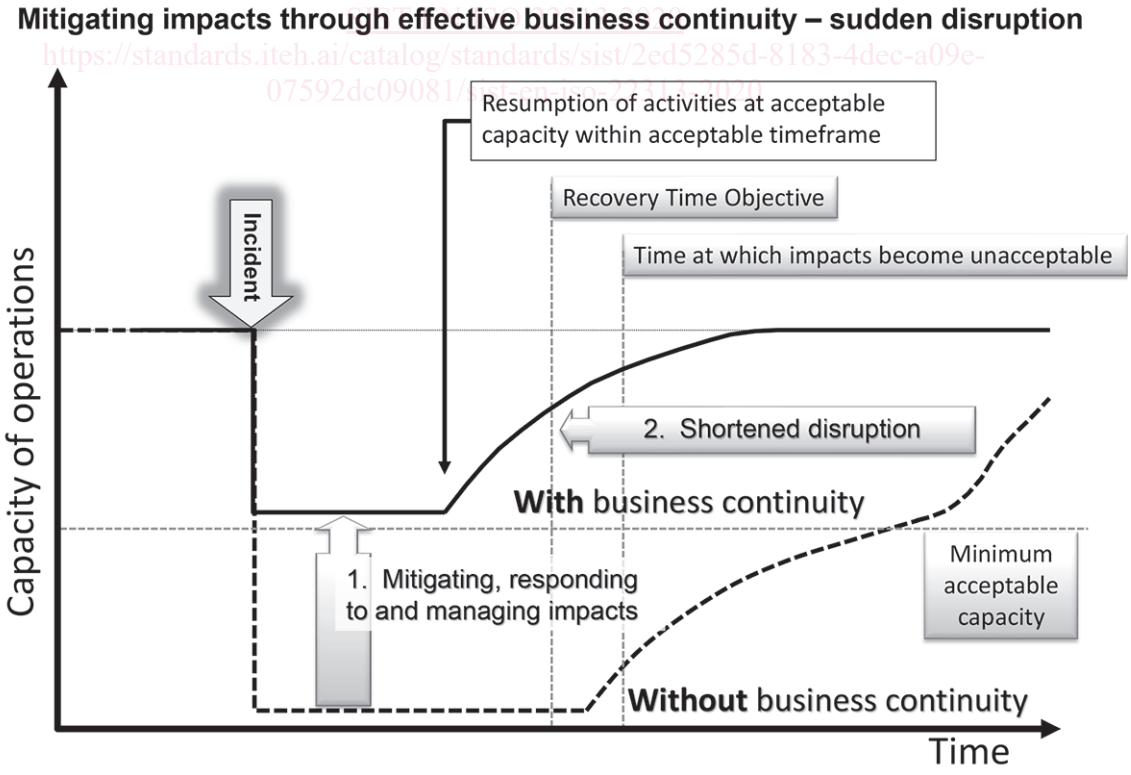

Figure 2 — Illustration of business continuity being effective for sudden disruption

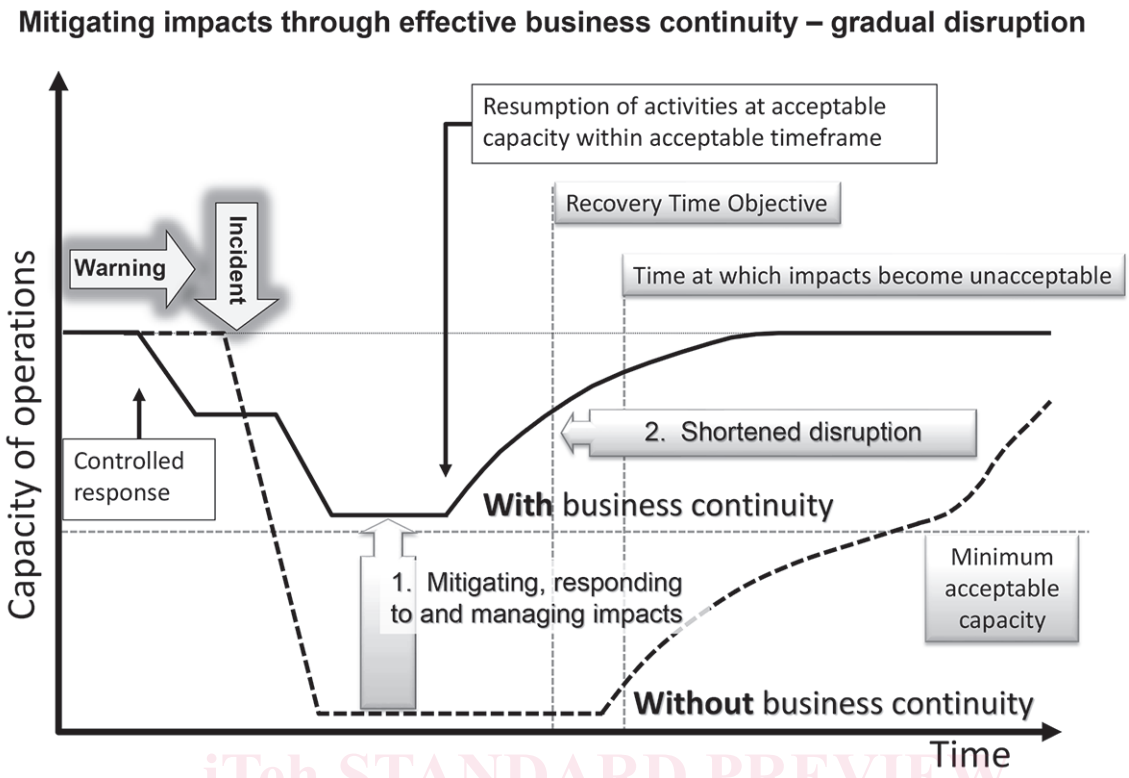

Figure 3 — Illustration of business continuity being effective for gradual disruption (e.g. approaching pandemic)

Security and resilience — Business continuity management systems — Guidance

1 Scope

This document provides guidance based on good international practice.

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 environment in which it operates, the size and structure of the organization and the requirements of its interested parties.

This document is generic and applicable to all sizes and types of organizations, including large, medium and small organizations operating in industrial, commercial, public and not-for-profit sectors that wish to:

a) implement and maintain a BCMS;

b) ensure conformance with the organization's business continuity policy;

c) continue delivery of products and services at acceptable predefined capacities during a disruption;

d) enhance their resilience;

e) make a self-determination and self-declaration of compliance with this document.

This document should not be used to assess an organization's ability to meet its own business continuity needs, nor any customer, legal or regulatory needs. Organizations wishing to do so can use the ISO 22301 requirements to demonstrate conformance to others or seek certification of its BCMS by an accredited third-party certification body.

2 Normative references

The following referenced documents are indispensable for the application 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*

ISO 22301, *Security and resilience — Business continuity management systems — Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and ISO 22301 apply.

3.1 Interpretation and meanings

For clarity and to improve readability and avoid unnecessary repetition, ISO 22301 and ISO 22313 have adopted the following conventions:

a) Rather than repeating the expression 'plan, establish, implement, operate, monitor, review, maintain and continually improve' in its entirety or using it with one or two of the words taken out:

   — For the BCMS, use 'implement and maintain';