SLOVENSKI STANDARD
oSIST prEN ISO 22301:2019

01-marec-2019

Varnost in vzdržljivost - Sistem vodenja neprekinjenosti poslovanja - Zahteve (ISO/DIS 22301:2019)

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

Sicherheit und Schutz des Gemeinwesens - Business Continuity Management System - Anforderungen (ISO/DIS 22301:2019)

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

Ta slovenski standard je istoveten z: **prEN ISO 22301**

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 22301:2019 **en,fr,de**

DRAFT INTERNATIONAL STANDARD

ISO/DIS 22301

ISO/TC **292**

Secretariat: **SIS**

Voting begins on:
2019-01-03

Voting terminates on:
2019-03-28

Security and resilience — Business continuity management systems — Requirements

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

ICS: 03.100.01; 03.100.70

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 22301:2019(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 22301 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 specifies the structure and requirements for implementing and maintaining an effective business continuity management system (BCMS).

An organization should develop business continuity that is appropriate to the magnitude and type of impact that it 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:

policy;

planning;

implementation and operation;

performance assessment;

management review;

continual improvement;

d) documented information supporting operational control and enabling performance evaluation.

0.2 Benefits of a BCMS

The 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:

— supporting its strategic objectives;

— creating a competitive advantage;

— protecting and enhancing its reputation and credibility;

— contributing to organizational resilience;

b) from a financial perspective:

— making business partners confident in its success;

— reducing legal and financial exposure;

— reducing direct and indirect costs of disruptions;

c) from the perspective of interested parties:

— protecting life, property and environment;

— considering the expectations of interested parties;

d) from an internal processes perspective:

— improving its capability to remain effective during disruptions;

— demonstrating proactive control of risks effectively and efficiently;

— addressing operational vulnerabilities.

0.3 The Plan-Do-Check-Act (PDCA) model

This document applies the "Plan-Do-Check-Act" (PDCA) model to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organization's BCMS.

This ensures a degree of consistency with other management systems standards, such as ISO 9001 *Quality management systems*, ISO 14001, *Environmental management systems*, ISO/IEC 27001, *Information security management systems*, ISO/IEC 20000-1, *Information technology – Service management*, and ISO 28000, *Specification for security management systems for the supply chain*, thereby supporting consistent and integrated implementation and operation with related management systems.

0.4 Components of PDCA in this document

In the PDCA model, Clause 4 through Clause 10 in this document cover the following components.

Clause 4 is a component of Plan. It introduces requirements necessary to establish the context of the BCMS as it applies to the organization, as well as needs, requirements, and scope.

Clause 5 is a component of Plan. It 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 is a component of Plan. It describes requirements as it relates to establishing strategic objectives and guiding principles for the BCMS as a whole.

Clause 7 is a component of Plan. It supports BCMS operations as they relate 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 is a component of Do. It defines business continuity needs, determines how to address them and develops the procedures to manage the organization during a disruption.

Clause 9 is a component of Check. It summarizes requirements necessary to measure business continuity performance, BCMS compliance with this document and management review.

Clause 10 is a component of Act. It identifies and acts on BCMS non-conformance 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 which apply to the use of this document, while 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 plan, establish, implement, operate, monitor, review, maintain and continually improve a management system to protect against, reduce the likelihood of occurrence, 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 an ability to continue delivery of products and services at 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

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

— ISO Online Browsing Platform: Available at http://www.iso.org/obp

— IEC Electropedia: Available at http://www.electropedia.org

3.1
activity
a set of one or more tasks with a defined output

[SOURCE: ISO 22300:2018, 3.1, modified. Note to entry deleted.]

3.2
audit
systematic, independent and documented *process* (3.40) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: The fundamental elements of an audit include the determination of the *conformity* (3.8) of an *object* (3.29) according to a *procedure* (3.39) carried out by *personnel* (3.35) not being responsible for the object audited.

Note 2 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 3 to entry: An internal audit is conducted by the organization or by an external party on its behalf. Internal audit can be for management (3.24) review (3.47) 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.

Note 4 to entry: External audits include those generally called 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 5 to entry: to entry "Audit evidence" and "audit criteria" are defined in ISO 19011.

[SOURCE: ISO 22300:2018, 3.13, modified. Notes to entry 5, 6 and 8 deleted.]

3.3
business continuity
capability of an *organization* (3.31) to continue delivery of *products and services* (3.41) within acceptable time frames at predefined capacity relating to a *disruption* (3.12)

[SOURCE: ISO 22300:2018, 3.24, modified.]

3.4
business continuity management system
BCMS
management system (3.25) for *business continuity* (3.3)

Note 1 to entry: The management system includes organizational structure, policies, *planning* (3.36) *activities* (3.1), responsibilities, *procedures* (3.39), *processes* (3.40) and resources

[SOURCE: ISO 22300:2018, 3.26, modified]

3.5
business continuity plan
documented information (3.13) that guides an *organization* (3.31) to respond to a *disruption* (3.12) and resume, recover and restore the delivery of products and services consistent with its business continuity objectives

[SOURCE: ISO 22300:2018, 3.27, modified. Note 1 to entry deleted.]

3.6
business impact analysis
process (3.40) of analyzing the impact (3.18) of a *disruption* (3.12) on the *organization* (3.31)

Note 1 to entry: The outcome is a statement and justification of *business continuity* (3.3) *requirements* (3.45).

[SOURCE: ISO 22300:2018, 3.29, modified. Note 1 to entry added.]

3.7
competence
ability to apply knowledge and skills to achieve intended results

[SOURCE: ISO 22300:2018, 3.44.]

3.8
conformity
fulfilment of a *requirement* (3.45)

[SOURCE: ISO 22300:2018, 3.45.]