INTERNATIONAL STANDARD

ISO 22301

Redline version
compares Second edition to
First edition

Security and resilience — Business continuity management systems — Requirements

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

Reference number
ISO 22301:redline:2019(E)

IMPORTANT

This marked-up version uses the following colour-coding in the marked-up text:

Text example 1 — Text has been added (in green)

~~Text example 2~~ — Text has been deleted (in red)

 — Graphic figure has been added

 — Graphic figure has been deleted

1.x ... — If there are changes in a clause/subclause, the corresponding clause/subclause number is highlighted in yellow in the Table of contents

DISCLAIMER

This marked-up version highlights the main changes in this edition of the document compared with the previous edition. It does not focus on details (e.g. changes in punctuation).

This marked-up version does not constitute the official ISO document and is not intended to be used for implementation purposes.

COPYRIGHT PROTECTED DOCUMENT

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.

~~International Standards are~~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 ~~rules given in~~editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

~~The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.~~

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.

~~ISO 22301~~This document was prepared by Technical Committee ISO/TC ~~223~~292, ~~*Societal security*~~*Security and resilience*.

This ~~corrected version of~~ second edition cancels and replaces the first edition (ISO 22301:2012 ~~incorporates the following corrections~~), which has been technically revised. The main changes compared with the previous edition are as follows:

— ~~first list in 6.1 changed from a numbered to an unnumbered list~~ISO's requirements for management system standards, which have evolved since 2012, have been applied;

— ~~commas added at the end of list items in 7.5.3 and 8.3.2~~requirements have been clarified, with no new requirements added;

— discipline-specific business continuity requirements are now almost entirely within Clause 8;

— ~~bibliography items [19] and [20] separated, which were merged in~~Clause 8 ~~the original~~has been re-structured to provide a clearer understanding of the key requirements;

— ~~font size adjusted in several places~~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 International Standard specifies requirements for setting up and managing an effective Business Continuity Management System (BCMS).

A BCMS emphasizes the importance of

— understanding the organization's needs and the necessity for establishing business continuity management policy and objectives;

— implementing and operating controls and measures for managing an organization's overall capability to manage disruptive incidents;

— monitoring and reviewing the performance and effectiveness of the BCMS; and

— continual improvement based on objective measurement.

A BCMS, like any other management system, has the following key components:

a) a policy;

b) people with defined responsibilities;

c) management processes relating to

1) policy;

2) planning;

3) implementation and operation;

4) performance assessment;

5) management review; and

6) improvement;

d) documentation providing auditable evidence; and

e) any business continuity management processes relevant to the organization.

Business continuity contributes to a more resilient society. The wider community and the impact of the organization's environment on the organization and therefore other organizations may need to be involved in the recovery process.

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

This International Standard 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.

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

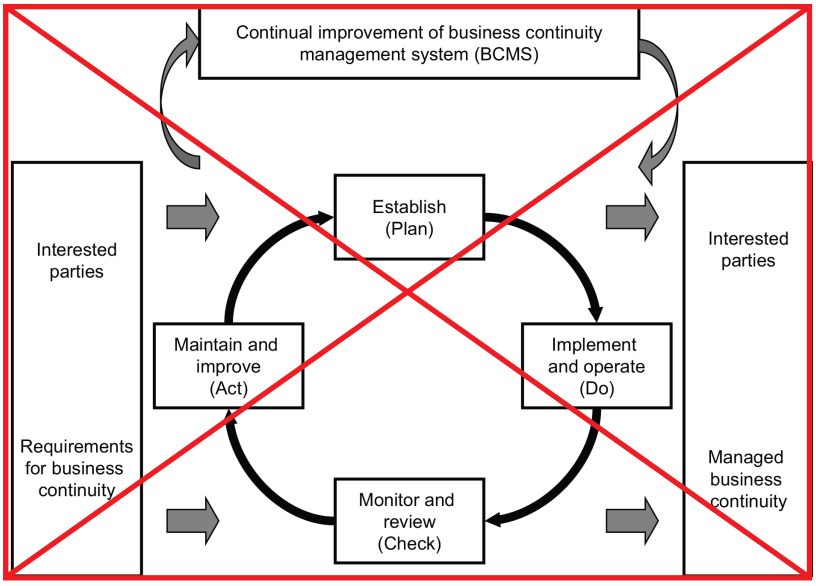

Figure 1 — PDCA model applied to BCMS processes

Table 1 — Explanation of PDCA model

Plan (Establish)	Establish business continuity policy, objectives, targets, 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 action, based on the results of management review and reappraising the scope of the BCMS and business continuity policy and objectives.

0.3 Components of PDCA in this International Standard

In the Plan-Do-Check-Act model as shown in Table 1, Clause 4 through Clause 10 in this International Standard 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. The content of Clause 6 differs from establishing risk treatment opportunities stemming from risk assessment, as well as business impact analysis (BIA) derived recovery objectives.

NOTE The business impact analysis and risk assessment process requirements are detailed in Clause 8.

— 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 documentation.

— Clause 8 is a component of Do. It defines business continuity requirements, determines how to address them and develops the procedures to manage a disruptive incident.

— Clause 9 is a component of Check. It summarizes requirements necessary to measure business continuity management performance, BCMS compliance with this International Standard and management's expectations, and seeks feedback from management regarding expectations.

— Clause 10 is a component of Act. It identifies and acts on BCMS non-conformance through corrective action.

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.

Security and resilience — Business continuity management systems — Requirements

1 Scope

This ~~International Standard for business continuity management~~document specifies requirements to ~~plan, establish, implement, operate, monitor, review, maintain and continually improve a documented~~implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from ~~disruptive incidents~~disruptions when they arise.

The requirements specified in this ~~International Standard~~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~~organization's operating environment and complexity.

~~It is not the intent of this International Standard to imply uniformity in the structure of a Business Continuity Management System (BCMS), but for an organization to design a BCMS that is appropriate to its needs and that meets its interested parties' requirements. These needs are shaped by legal, regulatory, organizational and industry requirements, the products and services, the processes employed, the size and structure of the organization, and the requirements of its interested parties.~~

This ~~International Standard~~document is applicable to all types and sizes of organizations that ~~wish to~~:

a) ~~establish,~~ implement, maintain and improve a BCMS~~;~~;

b) seek to ensure conformity with stated business continuity policy~~;~~;

c) ~~demonstrate conformity to others,~~need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption;

d) seek ~~certification/registration of its BCMS by an accredited third-party certification body, or~~to enhance their resilience through the effective application of the BCMS.

~~e) make a self-determination and self-declaration of conformity with this International Standard.~~

This ~~International Standard~~document can be used to assess an ~~organization's~~organization's ability to meet its own business continuity needs and obligations.

2 Normative references

The following documents~~, in whole or in part, are normatively referenced in this document and are indispensable for its application~~ are referred to in the text in such a way that some or all of their content constitutes requirements 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.

~~There are no normative references.~~

ISO 22300, *Security and resilience — Vocabulary*

3 Terms and definitions

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

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

— ISO Online browsing platform: available at https://www.iso.org/obp

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

NOTE The terms and definitions given below supersede those given in ISO 22300:2018.

3.1
activity
~~process or set of processes undertaken by an organization (or on its behalf) that produces or supports~~set of one or more ~~products and services~~tasks with a defined output

~~EXAMPLE Such processes include accounts, call centre, IT, manufacture, distribution.~~

[SOURCE: ISO 22300:2018, 3.1, modified — The definition has been replaced and the example has been deleted.]

3.2
audit
systematic, independent and documented ~~process~~*process* (3.26) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 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 2 to entry: An internal audit is conducted by the *organization* (3.21) itself, or by an external party on its behalf.

Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

Note 4 to entry: The fundamental elements of an audit include the determination of the *conformity* (3.7) of an object according to a procedure carried out by personnel not being responsible for the object audited.

Note 5 to entry: An internal audit can be for management review 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. External audits include 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 6 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards. The original definition has been modified by adding Notes 4 and 5 to entry.

3.3
business continuity
capability of ~~the organization~~an *organization* (3.21) to continue the delivery of ~~products or services~~ *products and services* (3.27)~~at acceptable predefined levels following disruptive incident~~ within acceptable time frames at predefined capacity during a *disruption* (3.10)

[SOURCE: ISO 22300:2018, 3.24, modified — The definition has been replaced.]

3.4
business continuity ~~management~~plan
~~holistic management process~~ *documented information* (3.11) that ~~identifies potential threats~~guides an *organization* (3.21) to ~~an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with~~respond to a *disruption* (3.10) ~~the capability of an effective response that safeguards the interests of~~and resume, recover and restore the delivery of *products and services* (3.27)~~its key stakeholders, reputation, brand and value-creating activities~~ consistent with its *business continuity* (3.3) *objectives* (3.20)

[SOURCE: ISO 22300:2018, 3.27, modified — The definition has been replaced and Note 1 to entry has been deleted.]