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)

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.

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.]

3.9
consequence
outcome of an *event* (**3.16**) affecting *objectives* (**3.30**)

Note 1 to entry: A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.

Note 2 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 3 to entry: Any consequence can escalate through cumulative effects.

[SOURCE: ISO 31000:2018, 3.6.**]**

3.10
continual improvement
recurring *activity* (3.1) to enhance *performance* (3.33)

[SOURCE: ISO 22300:2018, 3.48.]

3.11
corrective action
action to eliminate the cause of a *nonconformity* (3.28) and to prevent recurrence

Note 1 to entry: In the case of other undesirable outcomes, action is necessary to minimize or eliminate causes and to reduce *impact* (3.18) or prevent recurrence. Such actions fall outside the concept of "corrective action" in the sense of this definition.

[SOURCE: ISO 22300:2018, 3.54.]

3.12
disruption
incident (3.19), whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services (3.41) according to an *organization's* (3.31) *objectives* (3.30)

[SOURCE: ISO 22300:2018, 3.70, modified.]

3.13
documented information
information (3.20) required to be controlled and maintained by an *organization* (3.31) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and on any media, and from any source.

Note 2 to entry: Documented information can refer to:

the *management system* (3.25), including related *processes* (3.40);

information created in order for the organization to operate (documentation);

evidence of results achieved (*records* (3.43)).

[SOURCE: ISO 22300:2018, 3.72.]

3.14
effectiveness
extent to which planned *activities* (3.1) are realized and planned results achieved

[SOURCE: ISO 22300:2018, 3.76.]

3.15
emergency
sudden, urgent, usually unexpected occurrence or *event* (3.16) requiring immediate action

Note 1 to entry: An emergency is usually a *disruption* (3.12) or condition that can often be anticipated or prepared for, but seldom exactly foreseen.

[SOURCE: ISO 22300:2018, 3.77.]

3.16
event
occurrence or change of a particular set of circumstances

Note 1 to entry: An event can be one or more occurrences, and can have several causes and several *consequences* (3.9).

Note 2 to entry: An event can also be something that is expected which does not happen, or something that is not expected which does happen.

Note 3 to entry: An event can be a risk source.

[SOURCE: ISO 31000:2018, 3.5.]

3.17
exercise
process (3.40) to train for, assess, practice, and improve *performance* (3.33) in an *organization* (3.31)

Note 1 to entry: Exercises can be used for validating policies, plans, *procedures* (3.39), *training* (3.54), equipment, and inter-organizational agreements; clarifying and training *personnel* (3.35) in roles and responsibilities; improving inter-organizational coordination and communications; identifying gaps in resources; improving individual performance and identifying opportunities for improvement; and a controlled opportunity to practise improvisation. An exercise does not need an expectation of pass or fail.

Note 2 to entry: See also *test* (3.52).

[SOURCE: ISO 22300:2018, 3.83, modified, added 'An exercise does not need an expectation of pass or fail.']

3.18
impact
outcome of a disruption (3.12) affecting objectives (3.30)

[SOURCE: ISO 22300:2018, 3.107, modified.]

3.19
incident
event (3.16) that can be, or could lead to, a *disruption* (3.12), loss, *emergency* (3.15) or crisis

[SOURCE: ISO 22300:2018, 3.111, modified.]

3.20
information
data processed, organized and correlated to produce meaning

[SOURCE: ISO 22300:2018, 3.116.]

3.21
interested party
stakeholder
person or *organization* (3.31) that can affect, be affected by, or perceive themselves to be affected by a decision or *activity* (3.1)

EXAMPLE Customers, owners, *personnel* (3.35), providers, bankers, regulators, unions, partners or society that can include competitors or opposing pressure groups.

Note 1 to entry: A decision maker can be an interested party.

Note 2 to entry: Impacted communities and local populations are considered to be external interested parties.

[SOURCE: ISO 22300:2018, 3.124, modified. Example has been modified. Note 3 to entry has been deleted.]

3.22
internal audit
audit (3.2) conducted by, or on behalf of, an *organization* (3.31) itself for *management* (3.24) *review* (3.47) and other internal purposes, and which can form the basis for an organization's self-declaration of *conformity* (3.8)

Note 1 to entry: In many cases, particularly in smaller organizations, independence can be demonstrated by the freedom from responsibility for the *activity* (3.1) being audited.

[SOURCE: ISO 22300:2018, 3.126.]

3.23
likelihood
chance of something happening

Note 1 to entry: In *risk management* (3.50) terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Note 2 to entry: The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

[SOURCE: ISO 31000:2018, 3.7.]

3.24
management
coordinated *activities* (3.1) to direct and control an *organization* (3.31)

[SOURCE: ISO 22300:2018, 3.135.]

3.25
management system
set of interrelated or interacting elements of an *organization* (3.31) to establish *policies* (3.37) and *objectives* (3.30), and *processes* (3.40) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, *planning* (3.36) and operation.

Note 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

[SOURCE: ISO 22300:2018, 3.137. Note 3 modified to include 'may' instead of 'can'.]

3.26
measurement
process (3.40) to determine a value

[SOURCE: ISO 22300:2018, 3.143.]

3.27
monitoring
determining the status of a system, a *process* (3.40) or an *activity* (3.1)

[SOURCE: ISO 22300:2018, 3.147, modified.]

3.28
nonconformity
non-fulfilment of a *requirement* (3.45)

[SOURCE: ISO 22300:2018, 3.149.]

3.29
object
single and distinct entity that can be identified

[SOURCE: ISO 22300:2018, 3.151.]

3.30
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental objectives and can apply at different levels (such as strategic, organization-wide, project, product and *process* (3.40)).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of *business continuity management systems* (3.4), business continuity objectives are set by the organization, consistent with the business continuity *policy* (3.37), to achieve specific results.

[SOURCE: ISO 22300:2018, 3.30. Note 4 to entry has been modified to reflect BCMS.]

3.31
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.30)

Note 1 to entry: to entry : The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: For organizations with more than one operating unit, a single operating unit can be defined as an organization.

[SOURCE: ISO 22300:2018, 3.31.]

3.32
outsource (verb)
make an arrangement where an external *organization* (3.31) performs part of an organization's function or *process* (3.40)

Note 1 to entry: to entry : An external organization is outside the scope of the *management system* (3.25), although the outsourced function or process is within the scope.

[SOURCE: ISO 22300:2018, 3.160.]

3.33
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to the *management* (3.24) of *activities* (3.1), *processes* (3.40), *products and services* (3.41), systems or *organizations* (3.31).

[SOURCE: ISO 22300:2018, 3.157, modified – reference to 'products and services'.]

3.34
performance evaluation
process (3.40) to determine measurable results against the set criteria

[SOURCE: ISO 22300:2018, 3.168, modified, added 'against the set criteria', 'to determine, instead of 'of determining'.]

3.35
personnel
people working for and under the control of the *organization* (3.31)

Note 1 to entry: The concept of personnel includes, but is not limited to employees, part-time staff, and agency staff.

[SOURCE: ISO 22300:2018, 3.169.]

3.36
planning
part of *management* (**3.24**) focused on setting *business continuity* (**3.3**) *objectives* (**3.30**) and specifying necessary operational *processes* (**3.30**) and related resources to fulfil the business continuity objectives

[SOURCE: ISO 22300:2018, 3.170, modified to reflect 'business continuity'.]

3.37
policy
intentions and direction of an *organization* (3.31), as formally expressed by its *top management* (3.53)

[SOURCE: ISO 22300:2018, 3.171, modified to include comma.]

3.38
prioritized activity
activity (3.1) to which urgency is given in order to avoid unacceptable impacts to the business during a *disruption* (3.12)

[SOURCE: ISO 22300:2018, 3.176, modified.]

3.39
procedure
specified way to carry out an *activity* (3.1) or a *process* (3.40)

Note 1 to entry: Procedures can be documented or not.

Note 2 to entry: When a procedure is documented, the term "written procedure" or "documented procedure" is frequently used. The document that contains a procedure can be called a "procedure document".

[SOURCE: ISO 22300:2018, 3.179.]

3.40
process
set of interrelated or interacting *activities* (3.1) which transforms inputs into outputs

[SOURCE: ISO 22300:2018, 3.180, modified.]

3.41
product or service
output or outcome provided by an *organization* (3.31) to *interested parties* (3.21)

EXAMPLE Manufactured items, car insurance, community nursing

Note 1 to entry: [SOURCE: ISO 22300:2018, 3.181, modified.]

3.42
protection
measures that safeguard and enable an *organization* (**3.31**) to prevent or reduce the *impact* (3.18) of a potential *disruption* (3.12)

[SOURCE: ISO 22300:2018, 3.182.]

3.43
record
document stating results achieved or providing evidence of *activities* (3.1) performed

[SOURCE: ISO 22300:2018, 3.186.]

3.44
recovery
restoration and improvement, where appropriate, of operations, facilities, livelihoods or living conditions of affected *organizations* (**3.31**), including efforts to reduce *risk* (**3.48**) factors

[SOURCE: ISO 22300:2018, 3.187.]

3.45
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the *organization* (3.31) and *interested parties* (3.21) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, for example in *documented information* (3.13).

[SOURCE: ISO 22300:2018, 3.190.]

3.46
resilience
ability to absorb and adapt in a changing environment

[SOURCE: ISO 22300:2018, 3.192.]

3.47
review
activity (**3.1**) undertaken to determine the suitability, adequacy and *effectiveness* (**3.14**) of the *management s*ystem (**3.25**) and its component elements to achieve established *objectives* (**3.30**)

[SOURCE: ISO 22300:2018, 3.197.]

3.48
risk
effect of uncertainty on *objectives* (3.30)

Note 1 to entry: An effect is a deviation from the expected — it can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Objectives can have different aspects and categories and categories and can be applied at different levels .

Note 3 to entry: Risk is usually expressed in terms of risk sources, potential *events* (3.16) their *consequences* (3.9), and their *likelihood* (3.23).

[SOURCE: ISO 31000:2018, 3.1]

3.49
risk assessment
overall *process* (3.40) of risk identification, risk analysis and risk evaluation

Note 1 to entry: Risk assessment is described in detail in ISO 31000:2018.

[SOURCE: ISO 22300:2018, 3.203, modified – Note 1 to entry has been changed.]

3.50
risk management
coordinated *activities* (3.1) to direct and control an *organization* (3.31) with regard to *risk* (3.48).

[SOURCE: ISO 31000:2018, 3.2]

3.51
supply chain
two-way relationship of *organizations* (3.31), people, *processes* (3.40), logistics, *information* (3.20), technology and resources engaged in *activities* (3.1) and creating value from the sourcing of materials through the delivery of *products and services* (3.41)

Note 1 to entry: The supply chain may include vendors, subcontractors, manufacturing facilities, logistics providers, internal distribution centres, distributors, wholesalers and other entities that lead to the end user.

[SOURCE: ISO 22300:2018, 3.251, modified to 'products and services']

3.52
test
unique and particular type of *exercise* (3.17) which incorporates an expectation of a pass or fail element within the aim or *objectives* (3.30) of the exercise being planned

Note 1 to entry: The terms "test" and "testing" are not the same as "exercise" and "exercising".

[SOURCE: ISO 22300:2018, 3.257.]

3.53
top management
person or group of people who directs and controls an *organization* (3.31) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide *resources* within the organization.

Note 2 to entry: If the scope of the *management system* (3.25) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

[SOURCE: ISO 22300:2018, 3.263, modified. Notes 3, 4 and 5 to entry have been deleted.]

3.54
training
activities (**3.1**) designed to facilitate the learning and development of knowledge, skills and abilities, and to improve the *performance* (**3.33**) of specific tasks or roles

[SOURCE: ISO 22300:2018, 3.265.]

3.55
verification
confirmation, through the provision of evidence, that specified *requirements* (3.45) have been fulfilled

[SOURCE: ISO 22300:2018, 3.272.]

3.56
work environment
set of conditions under which work is performed

Note 1 to entry: Conditions include physical, social, psychological and environmental factors (such as temperature, recognition schemes, ergonomics and atmospheric composition).

[SOURCE: ISO 22300:2018, 3.276.]

4 Context of the organization

4.1 Understanding of the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its BCMS.

NOTE These issues will be influenced by the organization's overall objectives, its products and services and the amount and type of risk that it may or may not take.

4.2 Understanding the needs and expectations of interested parties

4.2.1 General

When establishing its BCMS, the organization shall determine:

a) the interested parties that are relevant to the BCMS;

b) the requirements of these interested parties.

4.2.2 Legal and regulatory requirements

The organization shall:

a) implement and maintain a process to identify, have access to, and assess the applicable legal and regulatory requirements related to the continuity of its products and services, processes, activities and resources, as well as the interests of relevant interested parties;

b) ensure that these applicable legal, regulatory and other requirements are taken into account in implementing and maintaining its BCMS;

c) document this information and keep it up-to-date.

4.3 Determining the scope of the business continuity management system

4.3.1 General

The organization shall determine the boundaries and applicability of the BCMS to establish its scope.

When determining this scope, the organization shall consider:

a) the external and internal issues referred to in 4.1;

b) the requirements referred to in 4.2.

The scope shall be available as documented information.

4.3.2 Scope of the BCMS

The organization shall:

a) consider its mission, goals, and internal and external obligations;

b) establish the parts of the organization to be included in the BCMS, taking into account its location(s), size, nature and complexity;

c) identify the products and services and their related processes, activities and resources to be included in the BCMS;

d) take into account interested parties' needs.

When defining the scope, the organization shall document and explain exclusions; any such exclusions shall not affect the organization's ability and responsibility to provide business continuity, as determined by the business impact analysis or risk assessment and applicable legal or regulatory requirements.

4.4 Business continuity management system

The organization shall establish, implement, maintain and continually improve a BCMS, including the processes needed and their interactions, in accordance with the requirements of this document.

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the BCMS by:

a) ensuring that the business continuity policy and business continuity objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the BCMS requirements into the organization's business processes;

c) ensuring that the resources needed for the BCMS are available;

d) communicating the importance of effective business continuity and conforming to the BCMS requirements;

e) ensuring that the BCMS achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the BCMS;

g) supporting other relevant management roles to demonstrate their leadership and commitment as it applies to their areas of responsibility;

h) promoting continual improvement.

NOTE Reference to “business” in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

5.2 Policy

5.2.1 Top management shall establish a business continuity policy that:

a) is appropriate to the purpose of the organization;

b) provides a framework for setting business continuity objectives;

c) includes a commitment to satisfy applicable requirements;

d) includes a commitment to continual improvement of the BCMS.

5.2.2 The business continuity policy shall:

a) be available as documented information;

b) be communicated within the organization;

c) be available to interested parties, as appropriate.

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

a) ensuring that the BCMS conforms to the requirements of this document;

b) reporting on the performance of the BCMS to top management.

6 Planning

6.1 Actions to address risks and opportunities

When planning for the BCMS, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) give assurance that the management system can achieve its intended outcome(s);

b) prevent, or reduce, undesired effects;

c) achieve continual improvement.

The organization shall plan:

a) actions to address these risks and opportunities,

b) how to:

1) integrate and implement the actions into its BCMS processes (see 8.1),

2) evaluate the effectiveness of these actions (see 9.1).

NOTE risks and opportunities in this subclause relate to the effectiveness of the management system. Risks related to disruption of the business are addressed in 8.2

6.2 Business continuity objectives and planning to achieve them

6.2.1 The organization shall establish business continuity objectives at relevant functions and levels.

The business continuity objectives shall:

a) be consistent with the business continuity policy;

b) be measurable (if practicable);

c) take into account applicable requirements;

d) be monitored;

e) be communicated;

f) be updated as appropriate.

The organization shall retain documented information on the business continuity objectives.

6.2.2 When planning how to achieve its business continuity objectives, the organization shall determine:

a) what will be done;

b) what resources will be required;

c) who will be responsible;

d) when it will be completed;

e) how the results will be evaluated.

6.3 Planning of changes to the BCMS

When the organization determines the need for changes to the BCMS, including those identified in clause 10 improvement, the changes shall be carried out in a planned manner.

The organization shall consider:

a) the purpose of the changes and their potential consequences;

b) the integrity of the BCMS;

c) the availability of resources;

d) the allocation or reallocation of responsibilities and authorities.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the BCMS.

7.2 Competence

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects its business continuity performance;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken;

d) retain appropriate documented information as evidence of competence.

NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the reassignment of currently employed persons; or the hiring or contracting of competent persons.

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

a) the business continuity policy;

b) their contribution to the effectiveness of the BCMS, including the benefits of improved business continuity performance;

c) the implications of not conforming with the BCMS requirements;

d) their own role and responsibilities before, during and after disruptions.

7.4 Communication

The organization shall determine the internal and external communications relevant to the BCMS including:

a) on what it will communicate;

b) when to communicate;

c) with whom to communicate;

d) how to communicate;

e) who will communicate.

7.5 Documented information

7.5.1 General

The organization's BCMS shall include:

a) documented information required by this document;

b) documented information determined by the organization as being necessary for the effectiveness of the BCMS.

NOTE The extent of documented information for a BCMS can differ from one organization to another due to:

the size of organization and its type of products and services, processes, activities and resources;

the complexity of processes and their interactions;

the competence of persons.

7.5.2 Creating and updating

When creating and updating documented information, the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic),

c) review and approval for suitability and adequacy.

7.5.3 Control of documented information

7.5.3.1 Documented information required by the BCMS and by this document shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed;

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

7.5.3.2 For the control of documented information, the organization shall address the following activities, as applicable:

a) distribution, access, retrieval and use;

b) storage and preservation, including preservation of legibility;

c) control of changes (e.g. version control);

d) retention and disposition.

Documented information of external origin determined by the organization to be necessary for the planning and operation of the BCMS shall be identified, as appropriate, and controlled.

NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information.

8 Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in 6.1, by:

a) establishing criteria for the processes;

b) implementing control of the processes in accordance with the criteria;

c) keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes and the supply chain are controlled.

8.2 Business impact analysis and risk assessment

8.2.1 General

The organization shall implement and maintain a process for analyzing business impact and assessing risks of disruption that establishes the context, defines criteria and evaluates the potential impact of a disruption.

NOTE The organization determines the order in which the business impact analysis and risk assessment are conducted.

8.2.2 Business impact analysis

The organization shall implement and maintain a process for determining business continuity priorities and requirements that:

a) defines impact categories and criteria relevant to the organization's context;

b) uses these impact categories and criteria for measuring impact;

c) identifies activities that support the provision of products and services;

d) analyses the impacts over time resulting from disruption of these activities;

e) identifies the time within which the impacts of not resuming activities would become unacceptable to the organization;

NOTE This may be referred to as maximum tolerable period of disruption (MTPD)

f) sets prioritized timeframes within the time identified in e) above for resuming disrupted activities at a specified minimum acceptable capacity;

NOTE This may be referred to as recovery time objective (RTO)

g) uses the business impacts to identify prioritized activities;

h) determines which resources are needed to support prioritized activities;

i) determines the dependencies and interdependencies of prioritized activities.

NOTE Outsource partners could be considered in accordance with ISO 22318.

8.2.3 Risk assessment

The organization shall implement and maintain a systematic risk assessment process.

NOTE This process can be made in accordance with ISO 31000.

The organization shall:

a) identify risks of disruption to the organization's prioritized activities and to their supporting resources;

b) systematically analyse risks of disruption;

c) evaluate risks of disruption which require treatment.

NOTE Risks in this subclause relate to the disruption of the business. Risks and opportunities related to the effectiveness of the management system are addressed in 6.1.

8.3 Business continuity strategies and solutions

8.3.1 General

The organization shall identify and select business continuity strategies based on the outputs from the business impact analysis and risk assessment. The business continuity strategies shall be comprised of one or more solutions.

8.3.2 Identification and selection of strategies and solutions

The organization shall identify and select appropriate business continuity strategies and solutions taking into consideration their associated costs for:

a) responding to disruptions;

b) continuing and recovering prioritized activities and their required resources to meet the delivery of products and services at the agreed capacity over time.

For the prioritized activities, the organization shall identify and select strategies and solutions considering business continuity objectives and the amount and type of risk that the organization may or may not take that:

a) reduce the likelihood of disruption;

b) shorten the period of disruption;

c) limit the impact of disruption on the organization's products and services.

8.3.3 Resource requirements

The organization shall determine the resource requirements to implement the selected business continuity solutions. The types of resources considered shall include but not be limited to:

a) people;

b) information and data;

c) physical infrastructure such as buildings, work places or other facilities and associated utilities;

d) equipment and consumables;

e) information and communication technology (ICT) systems;

f) transportation;

g) finance;

h) partners and suppliers.

8.3.4 Implementation of solutions

The organization shall implement selected business continuity solutions so they can be activated when needed.

8.4 Business continuity plans and procedures

8.4.1 General

The organization shall implement and maintain a structure that will enable timely warning and communication to relevant interested parties and provide plans and procedures to manage the organization during a disruption. The plans and procedures shall be used when required to execute business continuity solutions.

NOTE There are different types of procedures that comprise business continuity plans.

The procedures shall:

a) be specific regarding the immediate steps that are to be taken during a disruption;

b) be flexible to respond to changing internal and external conditions of a disruption;

c) focus on the impact of incidents that potentially lead to disruption;

d) be effective in minimizing impact through implementation of appropriate solutions;

e) assign roles and responsibilities for tasks within it.

8.4.2 Response structure

The organization shall implement and maintain a structure identifying one or more teams responsible for responding to disruptions.

The roles and responsibilities of each team and the relationships between the teams shall be clearly stated.

Collectively, the teams shall be prepared to:

a) assess the nature and extent of a disruption and its potential impact;

b) assess the impact against pre-defined thresholds that justify initiation of formal response;

c) activate an appropriate business continuity response;

d) plan actions that need to be undertaken;

e) establish priorities (using life safety as the first priority);

f) monitor the effects of the disruption and the organization's response;

g) activate the business continuity solutions;

h) communicate with relevant interested parties, authorities and the media.

For each team there shall be:

a) identified personnel and their associates with the necessary responsibility, authority and competence to perform their designated role;

b) documented procedures to guide their actions (see 8.4.4) including those for the activation, operation, coordination and communication of the response.

8.4.3 Warning and communication

8.4.3.1 The organization shall document and maintain procedures for:

a) communicating internally and externally to relevant interested parties, including what, when, with whom and how to communicate;

NOTE The organization may document and maintain procedures for how, and under what circumstances, the organization communicates with employees and their emergency contacts.

b) receiving, documenting and responding to communications from interested parties, including any national or regional risk advisory system or equivalent;

c) ensuring availability of the means of communication during a disruption;

d) facilitating structured communication with emergency responders;

e) details of the organization's media response following an incident, including a communications strategy;

f) recording details of the disruption, actions taken and decisions made.

8.4.3.2 Where applicable the following shall also be considered and implemented:

a) alerting interested parties potentially impacted by an actual or impending disruption;

b) assuring the appropriate coordination and communication between multiple responding organizations;

The communication and warning procedures shall be exercised as part of the organization's exercise programme referred to in 8.5.

8.4.4 Business continuity plans

8.4.4.1 The business continuity plans shall provide guidance and information that will assist the teams to respond to a disruption and assist the organization with response and recovery.

Collectively, the business continuity plans shall contain:

a) details of the actions that the teams will take in order to continue or recover prioritized activities within predetermined timeframes and to monitor the effects of the disruption and the organization's response to it;

b) reference to the pre-defined threshold and process for activating the response;

c) procedures to enable the delivery of products and services at agreed capacity to interested parties;

d) details to manage the immediate consequences of a disruption giving due regard to:

   1) the welfare of individuals;

   2) prevention of further loss or unavailability of prioritized activities;

   3) protection of the environment;

e) a process for standing down once the incident is over.

8.4.4.2 Each plan shall include:

a) purpose and scope, and objectives;

b) roles, responsibilities of the team that will implement the plan;

c) actions and resources to implement the solutions;

d) supporting information needed to activate (including activation criteria), operate, coordinate and communicate the team's actions;

e) internal and external interdependencies;

f) resource requirements;

g) reporting requirements.

Each plan shall be usable and available at the time and place at which it is required.

8.4.5 Recovery

The organization shall have documented processes to restore and return business activities from the temporary measures adopted to support normal business requirements during and after a disruption.

8.5 Exercise programme

The organization shall implement and maintain a programme of exercising and testing to validate over time the effectiveness of its business continuity strategies and solutions.

The organization shall conduct exercises and tests that:

a) are consistent with its business continuity objectives;

b) are based on appropriate scenarios that are well planned with clearly defined aims and objectives;

c) develop teamwork, competence, confidence and knowledge for those who have roles to perform in relation to disruptions;

d) taken together over time validate the whole of its business continuity strategies;

e) produce formalized post-exercise reports that contain outcomes, recommendations and actions to implement improvements;

f) are reviewed within the context of promoting continual improvement;

g) are performed at planned intervals and when there are significant changes within the organization or the context in which it operates.

The organization shall act on the results of its exercising and testing to implement changes and improvements.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.1.1 General

The organization shall determine:

a) what needs to be monitored and measured;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

c) when and by whom the monitoring and measuring shall be performed;

d) when and by whom the results from monitoring and measurement shall be analysed and evaluated.

The organization shall retain appropriate documented information as evidence of the results.

The organization shall evaluate the BCMS performance and the effectiveness of the BCMS.

9.1.2 Evaluation of business continuity plans, procedures and capabilities

The organization shall evaluate the suitability, adequacy and effectiveness of its business continuity plans, procedures and capabilities.

These evaluations shall be undertaken through periodic reviews, analysis, exercises, tests, post-incident reports and performance evaluations.

The organization shall periodically evaluate compliance with applicable legal and regulatory requirements, industry best practices, and conformance with its own business continuity policy and objectives.

The organization shall conduct evaluations at planned intervals after an incident or activation and when significant changes occur shall be updated in a timely manner.

9.2 Internal audit

9.2.1 The organization shall conduct internal audits at planned intervals to provide information on whether the BCMS:

a) conforms to:

   1) the organization's own requirements for its BCMS,

   2) the requirements of this document;

b) is effectively implemented and maintained.

9.2.1 The organization shall:

a) plan, establish, implement and maintain (an) audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;

b) define the audit criteria and scope for each audit;

c) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;

d) ensure that the results of the audits are reported to relevant management;

e) retain documented information as evidence of the implementation of the audit programme and the audit results.

9.3 Management review

9.3.1 General

Top management shall review the organization's BCMS, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

9.3.2 Management review input

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the BCMS;

c) information on the business continuity performance, including trends in:

   1) nonconformities and corrective actions;

   2) monitoring and measurement evaluation results;

   3) audit results;

d) feedback from interested parties;

e) the need for changes to the BCMS, including the policy and objectives;

f) procedures, and resources which could be used in the organization to improve the BCMS' performance and effectiveness;

g) information from the BIA and risk assessment;

h) risks or issues not adequately addressed in any previous risk assessment;

i) results of exercises and tests;

i) lessons learned and actions arising from near-misses and disruptions;

j) opportunities for continual improvement.

9.3.3 Management review outputs

9.3.3.1 The outputs of the management review shall include decisions related to continual improvement opportunities and the possible need for changes to the BCMS to improve its efficiency and effectiveness and include the following:

a) variations to the scope of the BCMS;

b) update of the business impact analysis, risk assessment, business continuity strategies and solutions, and business continuity plans;

c) modification of procedures and controls to respond to internal or external issues that may impact the BCMS;

d) how the effectiveness of controls will be measured.

9.3.3.2 The organization shall retain documented information as evidence of the results of management reviews, and:

a) communicate the results of management review to relevant interested parties;

b) take appropriate action relating to those results.

10 Improvement

10.1 Nonconformity and corrective action

10.1.1 When nonconformity occurs, the organization shall:

a) react to the nonconformity, and, as applicable:

   1) take action to control and correct it;

   2) deal with the consequences.

b) evaluate the need for action to eliminate the causes of the nonconformity in order that it does not recur or occur elsewhere, by:

   1) reviewing the nonconformity;

   2) determining the causes of the nonconformity;

   3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken;

e) make changes to the BCMS, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

10.1.2 The organization shall retain documented information as evidence of:

a) the nature of the nonconformities and any subsequent actions taken;

b) the results of any corrective action.

10.2 Continual improvement

The organization shall continually improve the suitability, adequacy or effectiveness of the BCMS.

The organization shall consider the results of analysis and evaluation, and the outputs from management review, to determine if there are needs or opportunities that shall be addressed as part of continual improvement.

NOTE The organization may use the processes of the BCMS such as leadership, planning and performance evaluation, to achieve improvement.

Bibliography

[1] ISO 9001, *Quality management systems — Requirements*

[2] ISO 14001, *Environmental management systems — Requirements with guidance for use*

[3] ISO 19011, *Guidelines for auditing management systems*

[4] ISO/IEC/TS 17021-6, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 6: Competence requirements for auditing and certification of business continuity management systems*

[5] ISO/IEC 20000-1, *Information technology — Service management — Part 1: Service management system requirements*

[6] ISO 22300, *Security and resilience — Vocabulary*

[7] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[8] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[9] ISO 28000, *Specification for security management systems for the supply chain*

[10] ISO 31000, *Risk management — Guidelines*

[11] ISO/IEC 31010, *Risk Management — Risk assessment techniques*

[12] SI 24001, *Security and continuity management systems — Requirements and guidance for use*, Standards Institution of Israel

[13] NFPA 1600, *Standard on disaster/emergency management and business continuity programs, National Fire Protection Association (USA)*

[14] Business Continuity Plan Drafting Guideline. Ministry of Economy, Trade and Industry, Japan, 2005

[15] *Business Continuity Guideline*, Central Disaster Management Council, Cabinet Office, Government of Japan, 2005

[16] ANSI/ASIS SPC. – 2011, Auditing management systems: Risk, *Resilience: Security, and Continuity –Guidance for Application*

[17] ANSI/ASIS/BSI BCM.01, *Business Continuity Management Systems: Requirements with Guidance for Use*