INTERNATIONAL STANDARD

ISO 22300

Third edition
2021-02

Security and resilience — Vocabulary

Sécurité et résilience — Vocabulaire

Reference number
ISO 22300:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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 of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience,* in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 391, *Societal and Citizen Security,* in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This third edition cancels and replaces the second edition (ISO 22300:2018), which has been technically revised. The main changes compared with the previous edition are as follows:

— terms have been added from recent published documents and documents transferred to ISO/TC 292;

— the terminological entries have been separated into subclauses by subject matter.

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

This document provides definitions of generic terms and subject-specific terms related to documents produced by ISO/TC 292. It covers the ISO 22300 family of standards as well as some documents in the ISO 28000 family of standards.

It aims to encourage a mutual and consistent understanding and use of uniform terms and definitions in processes and frameworks in the field of security and resilience.

This document can be applied as a reference by competent authorities, as well as by specialists involved in standardization systems, to better and more accurately understand relevant text, correspondences and communications.

The terms and definitions in 3.2, 3.3, 3.4 apply only to counterfeiting tax stamps standards, to supply chain standards or to CCTV standards, respectively, and do not apply generally.

Security and resilience — Vocabulary

1 Scope

This document defines terms used in security and resilience standards.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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/

3.1 Terms related to security and resilience

3.1.1
access
ability of the *rights holders* (3.1.214) to use or *benefit* (3.1.17) from a certain service or product

Note 1 to entry: Restrictions can be caused by distance to the source (e.g. water supply network does not reach a certain neighbourhood) or unaffordability (e.g. service is too costly for a certain household or group of people), among other reasons.

3.1.2
activity
set of one or more tasks with a defined output

3.1.3
adhesive
glue
chemical mixture that bonds two materials together

Note 1 to entry: It can be enabled by heat, pressure or chemistry.

3.1.4
affected area
location that has been impacted by a *disruptive event* (3.1.76) (incident, accident, disaster)

Note 1 to entry: The term is more relevant to immediate *evacuations* (3.1.92).

3.1.5
after-action report
final exercise report
document (3.1.77) that records, describes and analyses the actual *disruption* (3.1.75) or *exercise* (3.1.97), drawing on debriefs and reports from *observers* (3.1.163), and derives lessons from it

Note 1 to entry: The after-action report documents the results from the after-action *review* (3.1.211).

3.1.6
alert
part of *public warning* (3.1.197) that captures attention of first responders and *people at risk* (3.1.176) in a developing *emergency* (3.1.87) situation

3.1.7
all clear
message or signal that the danger is over

3.1.8
all-hazards
naturally occurring *event* (3.1.96), human induced event (both intentional and unintentional) and technology caused event with potential *impact* (3.1.118) on an *organization* (3.1.165), *community* (3.1.39) or society and the environment on which it depends

3.1.9
alternate worksite
work location, other than the primary location, to be used when the primary location is not accessible

3.1.10
analysis area
subject matter that has been selected to be *peer reviewed* (3.1.174)

EXAMPLE Governance of *risk management* (3.1.224), assessment of risk, financial capacity, urban development, climate change adaptation and ecosystem protection, institutional capacity, *community* (3.1.39) and societal capacity, economic and *business continuity* (3.1.19), *infrastructure* (3.1.128), public health, recovering and rebuilding.

3.1.11
analysis system
set of interconnecting parts that work together to form and deliver an *analysis area* (3.1.10)

3.1.12
area at risk
location that could be affected by a *disruptive event* (3.1.76) (incident, accident, disaster)

Note 1 to entry: The term is more relevant to preventative *evacuations* (3.1.92).

3.1.13
asset
anything that has value to an *organization* (3.1.165)

Note 1 to entry: Assets include but are not limited to human, physical, *information* (3.1.127), intangible and environmental *resources* (3.1.207).

3.1.14
audit
systematic, independent and documented *process* (3.1.190) 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* (3.1.134) (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* (3.1.165) 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* (3.1.44) of an *object* (3.1.161) according to a *procedure* (3.1.189) carried out by *personnel* (3.1.179) not being responsible for the object audited.

Note 5 to entry: An internal audit can be for *management* (3.1.144) *review* (3.1.211) 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* (3.1.2) 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.

3.1.15
auditor
person who conducts an *audit* (3.1.14)

[SOURCE: ISO 19011:2018, 3.15]

3.1.16
basic social services
set of services delivered in education, health and social areas, as a means to fulfil basic needs

3.1.17
benefit
measurable improvement resulting from the changes introduced as a result of a *peer review* (3.1.174)

Note 1 to entry: Benefits can be tangible or intangible, quantifiable or non-quantifiable, and financial or non-financial.

3.1.18
biodiversity
variability among living organisms from all sources including land, marine and other aquatic *ecosystems* (3.1.84) and the ecological complexes of which the organisms are part

Note 1 to entry: This includes diversity within species, between species and of ecosystems. Biodiversity is thus not only the sum of all ecosystems, species and genetic material, but rather represents the variability within and among them.

Note 2 to entry: Biodiversity can also be referred to as "biological diversity".

3.1.19
business continuity
capability of an *organization* (3.1.165) to continue the delivery of *products and services* (3.1.192) within acceptable time frames at predefined capacity during a *disruption* (3.1.75)

3.1.20
business continuity management
process (3.1.190) of implementing and maintaining *business continuity* (3.1.19)

3.1.21
business continuity management system
BCMS
part of the overall *management system* (3.1.146) that establishes, implements, operates, monitors, *reviews* (3.1.211), maintains and improves *business continuity* (3.1.19)

Note 1 to entry: The management system includes organizational structure, policies, planning activities, responsibilities, *procedures* (3.1.189), *processes* (3.1.190) and *resources* (3.1.207).

3.1.22
business continuity plan
documented information (3.1.78) that guides an *organization* (3.1.165) to respond to a *disruption* (3.1.75) and resume, recover and restore the delivery of *products and services* (3.1.192) consistent with its *business continuity* (3.1.19) *objectives* (3.1.162)

3.1.23
business continuity programme
ongoing *management* (3.1.144) and governance *process* (3.1.190) supported by *top management* (3.1.279) and appropriately resourced to implement and maintain *business continuity management* (3.1.20)

Note 1 to entry: In ISO 22301:2019, this term has been replaced by *business continuity management system* (3.1.21)

3.1.24
business impact analysis
process (3.1.190) of analysing the *impact* (3.1.118) over time of a *disruption* (3.1.75) on the *organization* (3.1.165)

Note 1 to entry: The outcome is a statement and justification of *business continuity* (3.1.19) *requirements* (3.1.204).

3.1.25
capacity
combination of all the strengths and *resources* (3.1.207) available within an *organization* (3.1.165), *community* (3.1.39) or society that can reduce the level of *risk* (3.1.215) or the effects of a *crisis* (3.1.60)

Note 1 to entry: Capacity can include physical, institutional, social, or economic means as well as skilled *personnel* (3.1.179) or attributes such as leadership and *management* (3.1.144).

3.1.26
carer
individual who provides support to a *vulnerable person* (3.1.293)

Note 1 to entry: Carers can be paid or unpaid providers of care.

3.1.27
cargo transport unit
road freight vehicle, railway freight wagon, freight container, road tank vehicle, railway tank wagon or portable tank

3.1.28
CCTV system
surveillance system comprised of cameras, recorders, interconnections and displays that is used to monitor activities in a store, a company or more generally a specific *infrastructure* (3.1.128) and/or a public place

3.1.29
challenge
contextual or environmental change that has the potential to *impact* (3.1.118) upon the ability and *capacity* (3.1.25) of an *urban system* (3.1.285) to address emerging risks and opportunities

3.1.30
civil protection
measures taken and systems implemented to preserve the lives and health of citizens, their properties and their environment from undesired *events* (3.1.96)

Note 1 to entry: Undesired events can include accidents, *emergencies* (3.1.85) and *disasters* (3.1.73).

3.1.31
civil society
wide range of individuals, groups of people, networks, movements, associations and *organizations* (3.1.165) that manifest and advocate for the interests of their members and others

Note 1 to entry: It can be based on philanthropic, cultural, religious, environmental or political values and convictions.

Note 2 to entry: This definition excludes for-profit companies and businesses, academia and all government-dependent entities.

3.1.32
civil society organization
CSO
formal association in which society voluntarily organizes around shared interests

Note 1 to entry: It includes political, cultural, environmental and faith-based organizations, as well as non-profit and non-governmental organizations.

Note 2 to entry: CSOs are institutionalized organizations, bearing some form of legal status, that represent particular groups of society and are involved in service delivery.

3.1.33
client
entity (3.1.91) that hires, has formerly hired, or intends to hire an *organization* (3.1.165) to perform *security operations* (3.1.249) on its behalf, including, as appropriate, where such an organization *subcontracts* (3.1.273) with another company or local forces

EXAMPLE Consumer, contractor, end-user, retailer, beneficiary, purchaser.

Note 1 to entry: A client can be internal (e.g. another division) or external to the organization.

3.1.34
colour blindness
total or partial inability of a person to differentiate between certain *hues* (3.1.113)

3.1.35
colour-code
set of colours used symbolically to represent particular meanings

3.1.36
command and control
activities (3.1.2) of target-orientated decision-making, including assessing the situation, *planning* (3.1.180), implementing decisions and controlling the effects of implementation on the *incident* (3.1.122)

Note 1 to entry: This *process* (3.1.190) is continuously repeated.

3.1.37
command and control system
system that supports effective *emergency management* (3.1.88) of all available *assets* (3.1.13) in a preparation, *incident response* (3.1.126), *continuity* (3.1.50) and/or *recovery* (3.1.201) *process* (3.1.190)

3.1.38
communication and consultation
continual and iterative *processes* (3.1.190) that an *organization* (3.1.165) conducts to provide, share or obtain *information* (3.1.127), and to engage in dialogue with *interested parties* (3.1.132) and others regarding the *management* (3.1.144) of *risk* (3.1.215)

Note 1 to entry: The information can relate to the existence, nature, form, *likelihood* (3.1.142), severity, *evaluation* (3.1.95), acceptability, treatment or other aspects of the management of risk and *security operations management* (3.1.250).

Note 2 to entry: Consultation is a two-way process of informed communication between an organization and its interested parties or others on an issue prior to making a decision or determining a direction on that issue. Consultation is:

— a process which impacts on a decision through influence rather than power; and

— an input to decision-making, not joint decision-making.

[SOURCE: ISO/Guide 73:2009, 3.2.1, modified — “interested parties and others” has replaced “stakeholders” and Note 1 to entry has been modified.]

3.1.39
community
group of associated *organizations* (3.1.165), individuals and groups sharing common interests

Note 1 to entry: Impacted communities are the groups of people and associated organizations affected by the provision of *security* (3.1.239) services, projects or operations.

3.1.40
community-based early warning system
community-based warning system
method to communicate *information* (3.1.127) to the public through established networks

Note 1 to entry: The warning system can consist of risk knowledge, *monitoring* (3.1.155) and warning service, dissemination and communication, and response capability to avoid, reduce *risks* (3.1.215) and prepare responses against *disaster* (3.1.73).

3.1.41
community vulnerability
characteristics and conditions of individuals, groups or *infrastructures* (3.1.128) that put them at *risk* (3.1.215) for the destructive effects of a *hazard* (3.1.110)

3.1.42
competence
ability to apply knowledge and skills to achieve intended results

Note 1 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.1.43
complexity
condition of an organizational system with many diverse and autonomous but interrelated and interdependent components or parts where those parts interact with each other and with external elements in multiple end non-linear ways

Note 1 to entry: Complexity is the characteristic of a system where behaviour cannot be determined only as the sum of individual variables behaviours.

3.1.44
conformity
fulfilment of a *requirement* (3.1.204)

Note 1 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.1.45
consequence
<outcome> outcome of an *event* (3.1.96) affecting *objectives* (3.1.162)

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 cascading and cumulative effects.

[SOURCE: ISO 31000:2018, 3.6]

3.1.46
consequence
<loss> loss of life, damage to property or economic disruption, including *disruption* (3.1.75) to transport systems, that can reasonably be expected as a result of an *attack* (3.2.4) on an *organization in the supply chain* (3.3.9) or by the use of the *supply chain* (3.1.271) as a weapon

3.1.47
context
external and internal factors to be taken into account when undertaking a capability assessment

Note 1 to entry: External context includes the following:

— the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

— key drivers and trends having an *impact* (3.1.118) on the *objectives* (3.1.162) of the *organization* (3.1.165);

— relationships with, and perceptions and values of, external *interested parties* (3.1.132).

Note 2 to entry: Internal context includes:

— the organization's mandate;

— business sensitivity;

— governance, organizational structure, roles and accountabilities;

— *resources* (3.1.207) and knowledge [e.g. capital, time, people, *processes* (3.1.190), systems and technologies];

— *organizational culture* (3.1.166).

3.1.48
contingency
possible future *event* (3.1.96), condition or eventuality

3.1.49
continual improvement
recurring *activity* (3.1.2) to enhance *performance* (3.1.177)

Note 1 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.1.50
continuity
strategic and tactical capability, pre-approved by *management* (3.1.144), of an *organization* (3.1.165) to plan for and respond to conditions, situations and *events* (3.1.96) in order to continue operations at an acceptable predefined level

Note 1 to entry: Continuity is the more general term for operational and *business continuity* (3.1.19) to ensure an organization's ability to continue operating outside of normal operating conditions. It applies not only to for-profit companies, but to organizations of all types, such as non-governmental, public interest and governmental.

3.1.51
control
measure that maintains and/or modifies *risk* (3.1.215)

Note 1 to entry: Controls include, but are not limited to, any *process* (3.1.190), *policy* (3.1.181), device, practice, or other conditions and/or actions which maintain and/or modify risk.

Note 2 to entry: Controls cannot always exert the intended or assumed modifying effect.

[SOURCE: ISO 31000:2018, 3.8]

3.1.52
cooperation
process (3.1.190) of working or acting together for common interests and values based on agreement

Note 1 to entry: The *organizations* (3.1.165) agree by contract or by other arrangements to contribute with their *resources* (3.1.207) to the *incident response* (3.1.126) but keep independence concerning their internal hierarchical structure.

3.1.53
coordination
way in which different *organizations* (3.1.165) (public or private) or parts of the same organization work or act together in order to achieve a common *objective* (3.1.162)

Note 1 to entry: Coordination integrates the individual response *activities* (3.1.2) of involved parties (including, for example, public or private organizations and government) to achieve synergy to the extent that the *incident response* (3.1.126) has a unified objective and coordinates activities through transparent *information* (3.1.127) sharing regarding their respective incident response activities.

Note 2 to entry: All organizations are involved in the *process* (3.1.190) to agree on a common incident response objective and accept to implement the strategies by this consensus decision-making process.

3.1.54
correction
action to eliminate a detected *nonconformity* (3.1.159)

[SOURCE: ISO 9000:2015, 3.12.3, modified — Notes 1 and 2 to entry have been deleted.]

3.1.55
corrective action
action to eliminate the cause(s) of a *nonconformity* (3.1.159) and to prevent recurrence

Note 1 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.1.56
counterfeit, verb
simulate, reproduce or modify a *material good* (3.1.149) or its packaging without authorization

3.1.57
counterfeit good
material good (3.1.149) imitating or copying an *authentic material good* (3.2.7)

3.1.58
countermeasure
action taken to lower the *likelihood* (3.1.142) of a *security threat scenario* (3.1.258) succeeding in its *objectives* (3.1.162), or to reduce the likely *consequences* (3.1.46) of a security threat scenario

3.1.59
coverage
capacity (3.1.25) of the *duty-bearer* (3.1.80) to provide a service or product

Note 1 to entry: It can be influenced by financial capacity, geospatial setting, and the normative and institutional frameworks.

3.1.60
crisis
unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, *assets* (3.1.13), property or the environment