INTERNATIONAL STANDARD

ISO 22300

Second edition
2018-02

Security and resilience — Vocabulary

Sécurité et résilience — Vocabulaire

Reference number
ISO 22300:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
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.

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

This second edition cancels and replaces the first edition (ISO 22300:2012), which has been technically revised.

The main changes compared to the previous edition are that terms have been added from recent published documents and documents transferred to ISO/TC 292.

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:

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

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

3.1
activity
process (3.180) or set of processes undertaken by an *organization* (3.158) (or on its behalf) that produces or supports one or more *products or services* (3.181)

EXAMPLE Accounts, call centre, IT, manufacture, distribution.

3.2
affected area
location that has been impacted by a *disaster* (3.69)

Note 1 to entry: The term is more relevant to immediate *evacuations* (3.80).

3.3
after-action report
document (3.71) which records, describes and analyses the *exercise* (3.83), drawing on debriefs and reports from *observers* (3.154), and derives lessons from it

Note 1 to entry: The after-action report documents the results from the after-action *review* (3.197).

Note 2 to entry: An after-action report is also called a final exercise report.

3.4
alert
part of *public warning* (3.183) that captures attention of first responders and *people at risk* (3.166) in a developing *emergency* (3.77) situation

3.5
all clear
message or signal that the danger is over

3.6
all-hazards
naturally occurring *event* (3.82), human induced event (both intentional and unintentional) and technology caused event with potential *impact* (3.107) on an *organization* (3.158), *community* (3.42) or society and the environment on which it depends

3.7
alternate worksite
work location, other than the primary location, to be used when the primary location is not accessible

3.8
appropriate law enforcement and other government officials
government and law enforcement *personnel* (3.169) that have specific legal jurisdiction over the *international supply chain* (3.127) or portions of it

3.9
area at risk
location that could be affected by a *disaster* (3.69)

Note 1 to entry: The term is more relevant to preventative *evacuations* (3.80).

3.10
asset
anything that has value to an *organization* (3.158)

Note 1 to entry: Assets include but are not limited to human, physical, *information* (3.116), intangible and environmental *resources* (3.193).

3.11
attack
successful or unsuccessful attempt(s) to circumvent an *authentication solution* (3.19), including attempts to imitate, produce or reproduce the *authentication elements* (3.17)

3.12
attribute data management system
ADMS
system that stores, manages and controls access of data pertaining to *objects* (3.151)

3.13
audit
systematic, independent and documented *process* (3.180) 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* (3.45) of an *object* (3.151) according to a *procedure* (3.179) carried out by *personnel* (3.169) 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 or a joint audit.

Note 3 to entry: Internal audits, sometimes called first-party audits, are conducted by, or on behalf of, the *organization* (3.158) itself for *management* (3.135) *review* (3.197) 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: When two or more *management systems* (3.137) are audited together, this is termed a combined audit.

Note 6 to entry: When two or more auditing organizations cooperate to audit a single auditee, this is termed a joint audit.

Note 7 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

Note 8 to entry: ISO 28000 specifies the *requirements* (3.190) for a *security management* (3.227) system.

[SOURCE: ISO 9000:2015, 3.13.1, modified — Note 5 to entry has been replaced and Notes 6 to 8 to entry have been added.]

3.14
auditor
person who conducts an *audit* (3.13)

[SOURCE: ISO 19011:2011, 3.8]

3.15
authentic material good
material good (3.139) produced under the control of the legitimate manufacturer, originator of the *goods* (3.98) or *rights holder* (3.198)

3.16
authentication
process (3.180) of corroborating an *entity* (3.79) or attributes with a specified or understood level of assurance

3.17
authentication element
tangible *object* (3.151), visual feature or *information* (3.116) associated with a *material good* (3.139) or its packaging that is used as part of an *authentication solution* (3.19)

3.18
authentication function
function performing *authentication* (3.16)

3.19
authentication solution
complete set of means and *procedures* (3.179) that allows the *authentication* (3.16) of a *material good* (3.139) to be performed

3.20
authentication tool
set of hardware and/or software system(s) that is part of an anti-counterfeiting solution and is used to control the *authentication element* (3.17)

3.21
authoritative source
official origination of an attribute which is also responsible for maintaining that attribute

3.22
authorized economic operator
party involved in the international movement of *goods* (3.98) in whatever function that has been approved by or on behalf of a national customs administration as conforming to relevant *supply chain* (3.251) security standards

Note 1 to entry: "Authorized economic operator" is a term defined in the *World Customs Organization* (WCO) (3.277) Framework of Standards.

Note 2 to entry: Authorized economic operators include, among others, manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses and distributors.

3.23
automated interpretation
process (3.180) that automatically evaluates authenticity by one or more components of the *authentication solution* (3.19)

3.24
business continuity
capability of an *organization* (3.158) to continue the delivery of *products or services* (3.181) at acceptable predefined levels following a *disruption* (3.70)

3.25
business continuity management
holistic *management* (3.135) *process* (3.180) that identifies potential *threats* (3.259) to an *organization* (3.158) and the *impact* (3.107) those threats, if realized, can cause on business operations, and provides a framework for building organizational *resilience* (3.192) with the capability of an effective response that safeguards the interests of key *interested parties* (3.124), reputation, brand and value-creating *activities* (3.1)

3.26
business continuity management system
BCMS
part of the overall *management system* (3.137) that establishes, implements, operates, monitors, *reviews* (3.197), maintains and improves *business continuity* (3.24)

Note 1 to entry: The management system includes organizational structure, policies, *planning* (3.170) *activities* (3.1), responsibilities, *procedures* (3.179), *processes* (3.180) and *resources* (3.193).

3.27
business continuity plan
documented *procedures* (3.179) that guide an organization to respond, recover, resume and restore itself to a pre-defined level of operation following a *disruption* (3.70)

Note 1 to entry: Typically this covers *resources* (3.193), services and *activities* (3.1) required to ensure the *continuity* (3.49) of critical business functions.

3.28
business continuity programme
ongoing *management* (3.135) and governance *process* (3.180) supported by *top management* (3.263) and appropriately resourced to implement and maintain *business continuity management* (3.25)

3.29
business impact analysis
process (3.180) of analysing *activities* (3.1) and the effect that a business *disruption* (3.70) can have upon them

3.30
business partner
contractor, supplier or service provider with whom an *organization* (3.158) contracts to assist the organization in its function as an *organization in the supply chain* (3.159)

3.31
capacity
combination of all the strengths and *resources* (3.193) available within an *organization* (3.158), *community* (3.42) or society that can reduce the level of *risk* (3.199) or the effects of a *crisis* (3.59)

Note 1 to entry: Capacity can include physical, institutional, social, or economic means as well as skilled *personnel* (3.169) or attributes such as leadership and *management* (3.135).

3.32
cargo transport unit
road freight vehicle, railway freight wagon, freight container, road tank vehicle, railway tank wagon or portable tank

3.33
certified client
organization (3.158) whose *supply chain* (3.251) *security management* (3.227) system has been certified/registered by a qualified third party

3.34
civil protection
measures taken and systems implemented to preserve the lives and health of citizens, their properties and their environment from undesired *events* (3.82)

Note 1 to entry: Undesired events can include accidents, emergencies and *disasters* (3.69).

3.35
client
entity (3.79) that hires, has formerly hired, or intends to hire an *organization* (3.158) to perform *security operations* (3.232) on its behalf, including, as appropriate, where such an organization subcontracts 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.

3.36
closed-circuit television system
CCTV system
surveillance system comprised of cameras, recorders, interconnections and displays that are used to monitor activities in a store, a company or more generally a specific *infrastructure* (3.117) and/or a public place

3.37
colour blindness
total or partial inability of a person to differentiate between certain *hues* (3.101)

3.38
colour-code
set of colours used symbolically to represent particular meanings

3.39
command and control
activities (3.1) of target-orientated decision making, including assessing the situation, *planning* (3.170), implementing decisions and controlling the effects of implementation on the *incident* (3.111)

Note 1 to entry: This *process* (3.180) is continuously repeated.

3.40
command and control system
system that supports effective *emergency management* (3.78) of all available *assets* (3.10) in a preparation, *incident response* (3.115), *continuity* (3.49) and/or *recovery* (3.187) *process* (3.180)

3.41
communication and consultation
continual and iterative *processes* (3.180) that an *organization* (3.158) conducts to provide, share or obtain *information* (3.116), and to engage in dialogue with *interested parties* (3.124) and others regarding the *management* (3.135) of *risk* (3.199)

Note 1 to entry: The information can relate to the existence, nature, form, *likelihood* (3.133), severity, *evaluation* (3.81), acceptability, treatment or other aspects of the management of risk and *security operations management* (3.233).

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 — In the definition, “stakeholders” has been changed to “interested parties and others” and Note 1 to entry has been modified.]

3.42
community
group of associated *organizations* (3.158), 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* (3.223) services, projects or operations.

3.43
community-based warning system
method to communicate *information* (3.116) to the public through established networks

3.44
competence
ability to apply knowledge and skills to achieve intended results

[SOURCE: ISO 9000:2015, 3.10.4, modified — Notes 1 and 2 to entry have been deleted.]

3.45
conformity
fulfilment of a *requirement* (3.190)

[SOURCE: ISO 9000:2015, 3.6.11, modified — Notes 1 and 2 to entry have been deleted.]

3.46
consequence
outcome of an *event* (3.82) affecting *objectives* (3.153)

Note 1 to entry: An event can lead to a range of consequences.

Note 2 to entry: A consequence can be certain or uncertain and can have positive or negative effects on objectives.

Note 3 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 4 to entry: Initial consequences can escalate through cumulative effects from one event setting off a chain of events.

Note 5 to entry: Consequences are graded in terms of the magnitude or severity of the *impacts* (3.107).

[SOURCE: ISO/Guide 73:2009, 3.6.1.3, modified — Note 5 to entry has been added.]

3.47
contingency
possible future *event* (3.82), condition or eventuality

3.48
continual improvement
recurring *activity* (3.1) to enhance *performance* (3.167)

[SOURCE: ISO 9000:2015, 3.3.2, modified — Notes 1 and 2 to entry have been deleted.]

3.49
continuity
strategic and tactical capability, pre-approved by *management* (3.135), of an *organization* (3.158) to plan for and respond to conditions, situations and *events* (3.82) 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* (3.24) 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.

3.50
conveyance
physical instrument of international trade that transports *goods* (3.98) from one location to another

EXAMPLE Box, pallet, *cargo transport unit* (3.32), cargo handling equipment, truck, ship, aircraft, railcar.

3.51
cooperation
process of working or acting together for common interests and values based on agreement

Note 1 to entry: The *organizations* (3.158) agree by contract or by other arrangements to contribute with their *resources* (3.193) to the *incident response* (3.115) but keep independence concerning their internal hierarchical structure.

3.52
coordination
way in which different *organizations* (3.158) (public or private) or parts of the same organization work or act together in order to achieve a common *objective* (3.153)

Note 1 to entry: Coordination integrates the individual response *activities* (3.1) of involved parties (including, for example, public or private organizations and government) to achieve synergy to the extent that the *incident response* (3.115) has a unified objective and coordinates activities through transparent *information* (3.116) sharing regarding their respective incident response activities.

Note 2 to entry: All organizations are involved in the *process* (3.180) to agree on a common incident response objective and accept to implement the strategies by this consensus decision-making process.

3.53
correction
action to eliminate a detected *nonconformity* (3.149)

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

3.54
corrective action
action to eliminate the cause of a *nonconformity* (3.149) 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* (3.107) or prevent recurrence. Such actions fall outside the concept of "corrective action" in the sense of this definition.

[SOURCE: ISO 9000:2015, 3.12.2, modified — Note 1 to entry has been replaced and Notes 2 and 3 to entry have been deleted.]

3.55
counterfeit
simulate, reproduce or modify a *material good* (3.139) or its packaging without authorization

3.56
counterfeit good
material good (3.139) imitating or copying an *authentic material good* (3.15)

3.57
countermeasure
action taken to lower the *likelihood* (3.133) of a *security threat scenario* (3.241) succeeding in its *objectives* (3.153), or to reduce the likely *consequences* (3.46) of a security threat scenario

3.58
covert authentication element
authentication element (3.17) that is generally hidden from the human senses and can be revealed by an informed person using a tool or by *automated interpretation* (3.23)

3.59
crisis
unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, *assets* (3.10), property or the environment

3.60
crisis management
holistic *management* (3.135) *process* (3.180) that identifies potential *impacts* (3.107) that threaten an *organization* (3.158) and provides a framework for building *resilience* (3.192), with the capability for an effective response that safeguards the interests of the organization's key *interested parties* (3.124), reputation, brand and value-creating *activities* (3.1), as well as effectively restoring operational capabilities

Note 1 to entry: Crisis management also involves the management of *preparedness* (3.172), *mitigation* (3.146) response, and *continuity* (3.49) or *recovery* (3.187) in the event of an *incident* (3.111), as well as management of the overall programme through *training* (3.265), rehearsals and *reviews* (3.197) to ensure the preparedness, response and continuity plans stay current and up-to-date.

3.61
crisis management team
group of individuals functionally responsible for directing the development and execution of the response and operational *continuity* (3.49) plan, declaring an operational *disruption* (3.70) or *emergency* (3.77)/*crisis* (3.59) situation, and providing direction during the *recovery* (3.187) *process* (3.180), both pre-and post-disruptive *incident* (3.111)

Note 1 to entry: The *crisis management team* (3.61) can include individuals from the *organization* (3.158) as well as immediate and first responders, and *interested parties* (3.124).

3.62
critical control point
CCP
point, step or *process* (3.180) at which controls can be applied and a *threat* (3.259) or *hazard* (3.99) can be prevented, eliminated or reduced to acceptable levels

3.63
critical customer
entity (3.79), the loss of whose business would threaten the survival of an *organization* (3.158)

3.64
critical product or service
resource (3.193) obtained from a supplier which, if unavailable, would disrupt an *organization's* (3.158) critical *activities* (3.1) and threaten its survival

Note 1 to entry: Critical products or services are essential resources to support an organization's high priority activities and *processes* (3.180) identified in its business impact analysis (BIA).

3.65
critical supplier
provider of *critical products or services* (3.64)

Note 1 to entry: This includes an "internal supplier", who is part of the same *organization* (3.158) as its customer.

3.66
criticality analysis
process (3.180) designed to systematically identify and evaluate an *organization's* (3.158) *assets* (3.10) based on the importance of its mission or function, the group of *people at risk* (3.166), or the significance of an *undesirable event* (3.268) or *disruption* (3.70) on its ability to meet expectations

3.67
custodian copy
duplicate that is subordinate to the *authoritative source* (3.21)

3.68
custody
period of time where an *organization in the supply chain* (3.159) is directly controlling the manufacturing, handling, processing and transportation of *goods* (3.98) and their related shipping *information* (3.116) within the *supply chain* (3.251)

3.69
disaster
situation where widespread human, material, economic or environmental losses have occurred which exceeded the ability of the affected *organization* (3.158), *community* (3.42) or society to respond and recover using its own *resources* (3.193)

3.70
disruption
event (3.82), whether anticipated (e.g. a labour strike or hurricane) or unanticipated (e.g. a blackout or earthquake), that causes an unplanned, negative deviation from the expected delivery of *products or services* (3.181) according to an *organization's* (3.158) *objectives* (3.153)

3.71
document
information (3.116) and the medium on which it is contained

Note 1 to entry: The medium can be paper, magnetic, electronic or optical computer disc, photograph or master sample, or a combination thereof.

Note 2 to entry: A set of documents, for example specifications and *records* (3.186), is frequently called "documentation".

[SOURCE: ISO 9000:2015, 3.8.5, modified — The example and Note 3 to entry has been deleted.]

3.72
documented information
information (3.116) required to be controlled and maintained by an *organization* (3.158) and the medium on which it is contained

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

Note 2 to entry: Documented information can refer to:

— the *management system* (3.137), including related *processes* (3.180);

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

— evidence of results achieved (*records* (3.186)).

[SOURCE: ISO 9000:2015, 3.8.6, modified — Note 3 to entry has been deleted.]

3.73
downstream
handling, processing and movement of *goods* (3.98) when they are no longer in the *custody* (3.68) of the *organization* in the *supply chain* (3.159)