DRAFT INTERNATIONAL STANDARD

ISO/DIS 22300

ISO/TC **292**	Secretariat: **SIS**
Voting begins on: **2020-03-17**	Voting terminates on: **2020-06-09**

Security and resilience — Vocabulary

Sécurité et résilience — Vocabulaire

ICS: 01.040.03; 03.100.01

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 22300:2020(E)

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

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

This third edition cancels and replaces the second edition (ISO 22300:2018), 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. The terms are also divided into normative and informative listings.

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 - Security and resilience. It aims to encourage a mutual and consistent understanding and use of uniform terms and definitions in processes and frameworks developed by its Working Groups.

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

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 General terms

3.1.1
activity
process (3.1.160) or set of processes undertaken by an *organization* (3.1.139) (or on its behalf) that produces or supports one or more *products or services* (3.1.162)

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

3.1.2
affected area
location that has been impacted by a *disaster* (3.1.55)

Note 1 to entry: The term is more relevant to immediate *evacuations* (3.1.167).

3.1.3
after-action report
document (3.1.57) which *records* (3.1.169), describes and analyses the *exercise* (3.1.172), drawing on debriefs and reports from observers (3.1.137), and derives lessons from it

Note 1 to entry: The after-action report documents the results from the after-action *review* (3.1.182).

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

3.1.4
alert
part of *public warning* (3.1.167) that captures attention of first responders and *people at risk* (3.1.147) in a developing *emergency* (3.1.63) situation

3.1.5
all clear
message or signal that the danger is over

3.1.6
all-hazards
naturally occurring *event* (3.1.71), human induced event (both intentional and unintentional) and technology caused event with potential *impact* (3.1.89) on an *organization* (3.1.139), *community* (3.1.26) or society and the environment on which it depends

3.1.7
area at risk
location that could be affected by a *disaster* (3.1.55)

Note 1 to entry: The term is more relevant to preventative *evacuations* (3.1.167).

3.1.8
asset
anything that has value to an *organization* (3.1.139)

Note 1 to entry: Assets include but are not limited to human, physical, *information* (3.1.98), intangible and environmental *resources* (3.1.176).

3.1.9
audit
systematic, independent and documented *process* (3.1.160) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

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

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

[SOURCE: ISO/IEC Directives, Part 1, Consolidated ISO Supplement, Procedures specific to ISO, Annex L, Appendix 2, 3.17, Tenth Edition 2019]

3.1.10
auditor
person who conducts an *audit* (3.1.9)

[SOURCE: ISO 19011:2011, 3.8]

3.1.11
business continuity
capability of an *organization* (3.1.139) to continue the delivery of *products or services* (3.1.162) at acceptable predefined levels following a *disruption* (3.1.56)

3.1.12
business continuity plan
documented *procedures* (3.1.159) that guide an *organization* (3.1.139) to respond, recover, resume and restore itself to a pre-defined level of operation following a *disruption* (3.1.56)

Note 1 to entry: Typically, this covers *resources* (3.1.176), services and *activities* (3.1.1) required to ensure the *continuity* (3.1.35) of critical business functions.

3.1.13
business continuity programme
ongoing *management* (3.1.114) and governance *process* (3.1.160) supported by *top management* (3.1.239) and appropriately resourced to implement and maintain business continuity management

3.1.14
business impact analysis
process (3.1.161) of analysing *activity* (3.1.1) and the effect that a business *disruption* (3.1.56) can have upon them

3.1.15
business partner
contractor, supplier or service provider with whom an *organization* (3.1.139) contracts to assist the organization in its function as an *organization in the supply chain* (3.3.6)

3.1.16
capacity
combination of all the strengths and *resources* (3.1.176) available within an *organization* (3.1.139, *community* (3.1.26) or society that can reduce the level of *risk* (3.1.182) or the effects of a *crisis* (3.1.44)

Note 1 to entry: Capacity can include physical, institutional, social, or economic means as well as skilled *personnel* (3.1.150) or *attributes* (3.2.7) such as leadership and *management* (3.1.114).

3.1.17
Carer
individual who provides support to a *vulnerable person* (3.1.246)

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

3.1.18
cargo transport unit
road freight vehicle, railway freight wagon, freight container, road tank vehicle, railway tank wagon or portable tank

3.1.19
civil protection
measures taken and systems implemented to preserve the lives and health of citizens, their properties and their environment from undesired *events* (3.1.71)

Note 1 to entry: Undesired events can include accidents, emergencies and *disasters* (3.1.55).

3.1.20
client
entity (3.1.66) that hires, has formerly hired, or intends to hire an *organization* (3.1.139) to perform *security operations* (3.1.214) 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.

3.1.21
colour blindness
total or partial inability of a person to differentiate between certain *hues* (3.1.87)

3.1.22
colour-code
set of colours used symbolically to represent particular meanings

3.1.23
command and control
activities (3.1.1) of target-orientated decision making, including assessing the situation, *planning* (3.1.151), implementing decisions and controlling the effects of implementation on the *incident* (3.1.93)

Note 1 to entry: This *process* (3.1.160) is continuously repeated.

3.1.24
command and control system
system that supports effective *emergency management* (3.1.64) of all available *assets* (3.1.8) in a preparation, *incident response* (3.1.97), *continuity* (3.1.35) and/or *recovery* (3.1.70) *process* (3.1.160)

3.1.25
communication and consultation
continual and iterative *processes* (3.1.160) that an *organization* (3.1.139 conducts to provide, share or obtain *information* (3.1.98), and to engage in dialogue with *interested parties* (3.1.103) and others regarding the *management* (3.1.114) of *risk* (3.1.182)

Note 1 to entry: The information can relate to the existence, nature, form, *likelihood* (3.1.112), severity, *evaluation* (3.1.70), acceptability, treatment or other aspects of the management of risk and *security operations management* (3.1.215).

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.]

3.1.26
community
group of associated *organizations* (3.1.139), 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* (3.1.205) services, projects or operations.

3.1.27
community-based warning system
method to communicate *information* (3.1.98) to the public through established networks

Note 1 to entry: The warning system can consist of risk knowledge, *monitoring* (3.1.129) and warning service, dissemination and communication, and response capability to avoid, reduce risks and prepare responses against *disaster* (3.1.55).

3.1.28
community vulnerability
characteristics and conditions of individuals, groups or *infrastructures* (3.1.99) that put them at *risk* (3.1.182) for the destructive effects of a *hazard* (3.1.85)

3.1.29
competence
ability to apply knowledge and skills to achieve intended results

[SOURCE: ISO/IEC Directives, Part 1, Consolidated ISO Supplement, Procedures specific to ISO, Annex L, Appendix 2, 3.10, Tenth Edition 2019]

3.1.30
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 behavior cannot be determined only as the sum of individual variables behaviors.

3.1.31
conformity
fulfilment of a *requirement* (3.1.173)

[SOURCE: ISO/IEC Directives, Part 1, Consolidated ISO Supplement, Procedures specific to ISO, Annex L, Appendix 2, 3.18, Tenth Edition 2019]

3.1.32
consequence
outcome of an *event* (3.1.71) affecting *objectives* (3.1.135)

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.]

3.1.33
contingency
possible future *event* (3.1.71), condition or eventuality

3.1.34
continual improvement
recurring activity to enhance *performance* (3.1.148)

[SOURCE: ISO/IEC Directives, Part 1, Consolidated ISO Supplement, Procedures specific to ISO, Annex L, Appendix 2, 3.21, Tenth Edition 2019]

3.1.35
continuity
strategic and tactical capability, pre-approved by *management* (3.1.114), of an *organization* (3.1.139) to plan for and respond to conditions, situations and *events* (3.1.71) 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* (3.1.11) 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.

3.1.36
conveyance
physical instrument of international trade that transports *goods* (3.1.84) from one location to another

EXAMPLE Box, pallet, *cargo transport unit* (3.1.18), cargo handling equipment, truck, ship, aircraft, railcar.

3.1.37
cooperation
process (3.1.160) of working or acting together for common interests and values based on agreement

Note 1 to entry: The *organizations* (3.1.139) agree by contract or by other arrangements to contribute with their *resources* (3.1.176) to the *incident response* (3.1.97) but keep independence concerning their internal hierarchical structure.

3.1.38
coordination
way in which different *organizations* (3.1.139) (public or private) or parts of the same organization work or act together in order to achieve a common *objective* (3.1.135)

Note 1 to entry: Coordination integrates the individual response *activities* (3.1.1) of involved parties (including, for example, public or private organizations and government) to achieve synergy to the extent that the *incident response* (3.1.97) has a unified objective and coordinates activities through transparent information (3.1.98) sharing regarding their respective incident response activities.

Note 2 to entry: All organizations are involved in the *process* (3.1.160) to agree on a common incident response objective and accept to implement the strategies by this consensus decision-making process.

3.1.39
correction
action to eliminate a detected *nonconformity* (3.1.133)

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

3.1.40
corrective action
action to eliminate the cause(s) of a *nonconformity* (3.1.133) and to prevent recurrence

[SOURCE: ISO/IEC Directives, Part 1, Consolidated ISO Supplement, Procedures specific to ISO, Annex L, Appendix 2, 3.20, Tenth Edition 2019]

3.1.41
counterfeit
simulate, reproduce or modify a *material good* (3.1.118) or its packaging without authorization

3.1.42
counterfeit good
material good (3.1.118) imitating or copying an *authentic material good* (3.2.9)

3.1.43
countermeasure
action taken to lower the *likelihood* (3.1.112) of a *security threat scenario* (3.1.223) succeeding in its *objectives* (3.1.135), or to reduce the likely *consequences* (3.1.32) of a security threat scenario

3.1.44
crisis
unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, *assets* (3.1.8), property or the environment

3.1.45
crisis management
holistic *management* (3.1.114) *process* (3..1.160) that identifies potential *impacts* (3.1.89) that threaten an *organization* (3.1.139) and provides a framework for building *resilience* (3.1.175), with the capability for an effective response that safeguards the interests of the organization's key *interested parties* (3.1.103), reputation, brand and value-creating *activities* (3.1.1), as well as effectively restoring operational capabilities

Note 1 to entry: Crisis management also involves the management of *preparedness* (3.1.153), *mitigation* (3.1.124) response, and *continuity* (3.1.35) or *recovery* (3.1.70) in the event of an *incident* (3.1.93), as well as management of the overall programme through *training* (3.1.240), rehearsals and *reviews* (3.1.182) to ensure the preparedness, response and continuity plans stay current and up-to-date.

3.1.46
crisis management team
group of individuals functionally responsible for directing the development and execution of the response and operational *continuity* (3.1.35) plan, declaring an operational *disruption* (3.1.56) or *emergency* (3.1.63) /*crisis* (3.1.44) situation, and providing direction during the *recovery* (3.1.70) *process* (3.1.160), both pre-and post-disruptive *incident* (3.1.93)

Note 1 to entry: The *crisis management team* (3.1.46) can include individuals from the *organization* (3.1.139) as well as immediate and first responders, and *interested parties* (3.1.103).

3.1.47
critical control point
CCP
point, step or *process* (3.1.160) at which controls can be applied and a threat (3.1.327) or *hazard* (3.1.85) can be prevented, eliminated or reduced to acceptable levels

