SLOVENSKI STANDARD
SIST EN ISO 22300:2018

01-maj-2018

Nadomešča:
SIST EN ISO 22300:2014

Varnost in vzdržljivost - Terminologija (ISO 22300:2018)

Security and resilience - Vocabulary (ISO 22300:2018)

Sicherheit und Resilienz - Terminologie (ISO 22300:2018)

Sécurité sociétale - Terminologie (ISO 22300:2018)

Ta slovenski standard je istoveten z: **EN ISO 22300:2018**

ICS:

01.040.03	Storitve. Organizacija podjetja, vodenje in kakovost. Uprava. Transport. Sociologija. (Slovarji)	Services. Company organization, management and quality. Administration. Transport. Sociology. (Vocabularies)
03.100.01	Organizacija in vodenje podjetja na splošno	Company organization and management in general

SIST EN ISO 22300:2018 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 22300

March 2018

ICS 01.040.03; 03.100.01

Supersedes EN ISO 22300:2014

English Version

Security and resilience - Vocabulary (ISO 22300:2018)

Sécurité et résilience - Vocabulaire (ISO 22300:2018)

Sicherheit und Resilienz - Terminologie (ISO 22300:2018)

This European Standard was approved by CEN on 22 January 2018.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword

This document (EN ISO 22300:2018) has been prepared by Technical Committee ISO/TC 292 “Security and resilience” in collaboration with Technical Committee CEN/TC 391 “Societal and citizen security” the secretariat of which is held by NEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by September 2018, and conflicting national standards shall be withdrawn at the latest by September 2018.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO 22300:2014.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 22300:2018 has been approved by CEN as EN ISO 22300:2018 without any modification.

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)