INTERNATIONAL STANDARD

ISO 22300

Third edition
2021-02

Security and resilience — Vocabulary

Sécurité et résilience — Vocabulaire

Reference number
ISO 22300:2021(E)

COPYRIGHT PROTECTED DOCUMENT

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

3.1.61
crisis management
holistic *management* (3.1.144) *process* (3.1.190) that identifies potential *impacts* (3.1.118) that threaten an *organization* (3.1.165) and provides a framework for building *resilience* (3.1.206), with the capability for an effective response that safeguards the interests of the organization's key *interested parties* (3.1.132), reputation, brand and value-creating *activities* (3.1.2), as well as effectively restoring operational capabilities

Note 1 to entry: Crisis management also involves the management of *preparedness* (3.1.182), *mitigation* (3.1.154) response, and *continuity* (3.1.50) or *recovery* (3.1.201) in the event of an *incident* (3.1.122), as well as management of the overall programme through *training* (3.1.280), rehearsals and *reviews* (3.1.211) to ensure the preparedness, response and continuity plans stay current and up to date.

3.1.62
crisis management team
group of individuals functionally responsible for directing the development and execution of the response and operational *continuity* (3.1.50) plan, declaring an operational *disruption* (3.1.75) or *emergency* (3.1.87)/*crisis* (3.1.60) situation, and providing direction during the *recovery* (3.1.201) *process* (3.1.190), both pre-and post-disruptive *incident* (3.1.122)

Note 1 to entry: The crisis management team can include individuals from the *organization* (3.1.165) as well as immediate and first responders and *interested parties* (3.1.132).

3.1.63
critical control point
CCP
point, step or *process* (3.1.190) at which *controls* (3.1.51) can be applied and a *threat* (3.1.277) or *hazard* (3.1.110) can be prevented, eliminated or reduced to acceptable levels

3.1.64
critical customer
entity (3.1.91), the loss of whose business would threaten the survival of an *organization* (3.1.165)

3.1.65
critical facility
physical structure, network or other *asset* (3.1.13) that provide services that are essential to the social and economic functioning of a *community* (3.1.39) or society

3.1.66
critical indicator
quantitative, qualitative or descriptive measure used to assess the *hazard* (3.1.110) being monitored to identify the potential for the development of an *incident* (3.1.122), accident or *emergency* (3.1.87)

Note 1 to entry: Critical indicators provide *information* (3.1.127) about the most important integral characteristics of the structural state of a *facility* (3.1.105).

3.1.67
critical product and service
resource (3.1.207) obtained from a supplier, which, if unavailable, would disrupt an *organization's* (3.1.165) critical *activities* (3.1.2) 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* (3.1.190) identified in its *business impact analysis* (3.1.24).

3.1.68
critical supplier
provider of *critical products or services* (3.1.50)

Note 1 to entry: This includes an "internal supplier", who is part of the same *organization* (3.1.165) as its customer.

3.1.69
criticality analysis
process (3.1.190) designed to systematically identify and evaluate an *organization's* (3.1.165) *assets* (3.1.13) based on the importance of its mission or function, the group of *people at risk* (3.1.176), or the significance of an *undesirable event* (3.1.281) or *disruption* (3.1.75) on its ability to meet expectations

3.1.70
critically
of essential importance with respect to *objectives* (3.1.162) and/or outcomes

3.1.71
data analysis
systematic investigation of relevant, evidence-based *information* (3.1.127) obtained in *monitoring* (3.1.155) the *process* (3.1.190) and its flow in a real or planned system

3.1.72
decentralized authority
local authorities, distinct from the state's administrative authorities, that have a degree of self-government, elaborated in the framework of the law, with their own powers, *resources* (3.1.207) and capacities to meet responsibilities, and with legitimacy underpinned by representative, elected local democratic structures that determine how power is exercised and that make local authorities accountable to citizens in their jurisdiction

3.1.73
disaster
situation where widespread human, material, economic or environmental losses have occurred that exceeded the ability of the affected *organization* (3.1.165), *community* (3.1.39) or society to respond and recover using its own *resources* (3.1.207)

3.1.74
disaster risk reduction
policy (3.1.181) aimed at preventing new and reducing existing disaster risk and managing *residual risk* (3.1.205), all of which contribute to strengthening *resilience* (3.1.206) and therefore to the achievement of sustainable development

3.1.75
disruption
incident (3.1.122), whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of *products and services* (3.1.192) according to an *organization's* (3.1.165) *objectives* (3.1.162)

3.1.76
disruptive event
occurrence or change that interrupts planned *activities* (3.1.2), operations or functions, whether anticipated or unanticipated

3.1.77
document
information (3.1.127) 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* (3.1.200), is frequently called "documentation".

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

3.1.78
documented information
information (3.1.127) required to be controlled and maintained by an *organization* (3.1.165) 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* (3.1.146), including related *processes* (3.1.190);

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

— evidence of results achieved (*records* (3.1.200)).

Note 3 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.1.79
drill
activity (3.1.2) that practises a particular skill and often involves repeating the same thing several times

EXAMPLE A fire drill to practise safely evacuating a building on fire.

3.1.80
duty-bearer
individual who has a particular obligation or responsibility to respect, promote and realize *human rights* (3.1.115), and to abstain from human rights violations

Note 1 to entry: The term is most commonly used to refer to state actors, but non-state actors can also be considered as duty-bearers.

Note 2 to entry: Depending on the *context* (3.1.47), individuals (e.g. parents), local *organizations* (3.1.165), private companies, aid donors and international institutions can also be duty-bearers.

3.1.81
duty of care
moral or legal obligation to ensure the safety, well-being or interests of others

3.1.82
early warning
provision of *information* (3.1.127) through local networks, allowing affected individuals to take action to avoid or reduce *risks* (3.1.215) and to prepare responses

3.1.83
economic diversity
extent to which economic *activity* (3.1.2) of a given defined geography is distributed among a number of categories such as industries, sectors, skill levels and employment levels

3.1.84
ecosystem
dynamic complex of plant, animal and micro-organism communities and their non-living environment (e.g. soil, air, sunlight) interacting as a functioning unit of nature

Note 1 to entry: Everything that lives in an ecosystem is dependent on the other species and elements that are also part of that ecological community.

[SOURCE: ISO 14055-1:2017, 3.1.1, modified — "(e.g. soil, air, sunlight) interacting as a functioning unit of nature" has replaced "interacting as a functional unit" and Note 1 to entry has been added.]

3.1.85
ecosystem services
benefit (3.1.17) people obtain from *ecosystems* (3.1.84)

Note 1 to entry: These include: provisioning services such as food, water, timber and fibre; regulating services that affect the climate, floods, disease, waste generation and water quality; cultural services that provide recreational, aesthetic and spiritual benefits and supporting services such as soil formation, photosynthesis and nutrient cycling.

[SOURCE: ISO 14055-1:2017, 3.1.2, modified — Note 1 to entry has been revised and expanded.]

3.1.86
effectiveness
extent to which planned *activities* (3.1.2) are realized and planned results achieved

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

3.1.87
emergency
sudden, urgent, usually unexpected occurrence or *event* (3.1.96) requiring immediate action

Note 1 to entry: An emergency is usually a *disruption* (3.1.75) or condition that can often be anticipated or prepared for, but seldom exactly foreseen.

3.1.88
emergency management
overall approach for preventing *emergencies* (3.1.63) and managing those that occur

Note 1 to entry: In general, emergency management utilizes a *risk management* (3.1.224) approach to *prevention* (3.1.183), *preparedness* (3.1.182), response and *recovery* (3.1.201) before, during and after potentially destabilizing *events* (3.1.96) and/or *disruptions* (3.1.75).

3.1.89
emergency management capability
overall ability to effectively manage *prevention* (3.1.183), *preparedness* (3.1.182), response and *recovery* (3.1.201) before, during and after potentially destabilizing or *disruptive events* (3.1.76)

3.1.90
employee assistance programme
contracted support service provided to *organizations* (3.1.165) to assist them in addressing productivity issues, and to assist employees in identifying and resolving personal concerns, including health, marital, family, financial, alcohol, drug, legal, emotional, stress or other personal issues that could affect job *performance* (3.1.177)

Note 1 to entry: Adapted from the International Employee Assistance Professionals Association (EAPA).

3.1.91
entity
something that has a separate and distinct existence and that can be identified within *context* (3.1.47)

Note 1 to entry: An entity can be a human, *organization* (3.1.165), physical *object* (3.1.161), class of objects or intangible object.

3.1.92
evacuation
organized, phased and supervised movement of people from dangerous or potentially dangerous areas to places of safety

3.1.93
evacuation command
series of orders to evacuate people

3.1.94
evacuation drill
activity (3.1.2) that practises a particular skill related to *evacuation* (3.1.92) and often involves repeating the same thing several times

EXAMPLE A *drill* (3.1.79) to practise safely evacuating a neighbourhood or village from a *landslide* (3.1.141).

3.1.95
evaluation
systematic *process* (3.1.190) that compares the result of *measurement* (3.1.152) to recognised criteria to determine the discrepancies between intended and actual *performance* (3.1.177)

Note 1 to entry: Gaps in performance are inputs into the *continual improvement* (3.1.49) process.

3.1.96
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* (3.1.45).

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* (3.1.230).

[SOURCE: ISO 31000:2018, 3.5]

3.1.97
exercise
process (3.1.190) to train for, assess, practise, and improve *performance* (3.1.177) in an *organization* (3.1.165)

Note 1 to entry: Exercises can be used for validating *policies* (3.1.182), plans, *procedures* (3.1.189), *training* (3.1.280), equipment, and inter-organizational agreements; clarifying and training *personnel* (3.1.179) in roles and responsibilities; improving inter-organizational *coordination* (3.1.53) and communications; identifying gaps in *resources* (3.1.207); improving individual performance and identifying opportunities for improvement; and a controlled opportunity to practise *improvisation* (3.1.121). An exercise does not need an expectation of pass or fail.

Note 2 to entry: See also *test* (3.1.275).

3.1.98
exercise annual plan
document (3.1.77) in which the *exercise* (3.1.97) *policy* (3.1.181) plan has been translated to exercise goals and exercises, and in which an *exercise programme* (3.1.100) for a certain year is reflected

3.1.99
exercise coordinator
person responsible for *planning* (3.1.180), conducting and evaluating *exercise* (3.1.97) *activities* (3.1.2)

Note 1 to entry: In larger exercises, this function can include several people/staff and can be called “exercise control”.

Note 2 to entry: Some countries use a term such as “exercise director” or similar instead of “exercise coordinator”.

Note 3 to entry: The exercise coordinator role is also responsible for the *cooperation* (3.1.52) among internal and external *entities* (3.1.66).

3.1.100
exercise programme
series of *exercise* (3.1.97) *activities* (3.1.2) designed to meet an overall *objective* (3.1.162) or goal

3.1.101
exercise programme manager
person responsible for *planning* (3.1.180) and improving the *exercise programme* (3.1.100)

3.1.102
exercise project team
group of individuals responsible for *planning* (3.1.180), conducting and evaluating an *exercise* (3.1.97) project

3.1.103
exercise safety officer
person tasked with ensuring that any actions during the *exercise* (3.1.97) are performed safely

Note 1 to entry: In larger exercises, involving multiple functions, more than one safety officer can be assigned.

3.1.104
external attack
attack (3.2.4) perpetrated by persons or entities that are not directly or indirectly linked with the legitimate manufacturer, originator of the good or *rights holder* (3.1.214)

3.1.105
facility
plant, machinery, property, building, transportation units at sea/land/airport, and other items of *infrastructure* (3.1.128) or plant and related systems that have a distinct and quantifiable business function of service

Note 1 to entry: A facility can have formal boundaries as defined by, for example, legislation.

3.1.106
forensic
related to, or used in, courts of law

Note 1 to entry: This applies to *video-surveillance* (3.1.289) used to produce legal evidence.

3.1.107
full-scale exercise
exercise (3.1.97) that involves multiple *organizations* (3.1.165) or functions and includes actual *activities* (3.1.2)

3.1.108
functional exercise
exercise (3.1.97) to train for, assess, practise and improve the *performance* (3.1.177) of single functions designed to respond to and recover from an unwanted *event* (3.1.96)

Note 1 to entry: Functions can include an emergency operations centre (EOC) team, a *crisis management team* (3.1.62) or firefighters decontaminating mock victims.

3.1.109
geo-location
specific location defined by one of several means to represent latitude, longitude, elevation above sea level and coordinate system

Note 1 to entry: Geo-location generally means the meaningful specification of the position of a point or *object* (3.1.161) on the earth. The term itself does not carry a prescription of the coordinate system to be used. Additional *attributes* (3.2.5) associated with a geo-location are not a part of a geo-location specification.

3.1.110
hazard
source (3.1.266) of potential harm

Note 1 to entry: Hazard can be a *risk source* (3.1.230).

[SOURCE: ISO/Guide 73:2009, 3.5.1.4]

3.1.111
hazard monitoring function
activities (3.1.2) to obtain evidence-based *information* (3.1.127) on *hazards* (3.1.110) in a defined area used to make decisions about the need for *public warning* (3.1.197)

3.1.112
host
entity (3.1.91) that receives feedback from a *reviewer* (3.1.213) as part of a *peer review* (3.1.174)

Note 1 to entry: The entity can be an *organization* (3.1.165), *partnership* (3.1.173), *community* (3.1.39), city, region, country or other body.

3.1.113
hue
attribute (3.2.5) of a visual sensation where an area appears to be similar to one of the perceived colours, red, yellow, green, and blue, or to a combination of two of them

3.1.114
human interpretation
authenticity as evaluated by an *inspector* (3.2.24)

3.1.115
human rights
rights inherent to all human beings, whatever their nationality, place of residence, sex, national or ethnic origin, colour, religion, language or any other status

Note 1 to entry: People are all equally entitled to their human rights without discrimination.

Note 2 to entry: Human rights are: interrelated, universal and inalienable; interdependent and indivisible; equal and non-discriminatory; and both rights and obligations.

3.1.116
human rights risk analysis
HRRA
human rights risk assessment
human rights impact assessment
human rights risk and impact assessment
process (3.1.190) to identify, analyse, evaluate and *document* (3.1.77) human rights-related *risks* (3.1.215) and their *impacts* (3.1.118), in order to manage risk and to mitigate or prevent adverse *human rights* (3.1.115) impacts and legal infractions

Note 1 to entry: The HRRA is part of the *organization's* (3.1.165) *requirement* (3.1.204) to undertake human rights due diligence to identify, prevent, mitigate and account for how it addresses impacts on human rights.

Note 2 to entry: The HRRA is framed by relevant international human rights principles and conventions and forms a fundamental part of the organization's overall *risk assessment* (3.1.219).

Note 3 to entry: The HRRA includes an analysis of the severity of actual and potential human rights impacts that the organization can cause or contribute to through its *security operations* (3.1.249), or which can be linked directly to the organization's operations, projects or services through its business relationships. The HRRA process should include consideration of the operational context, draw on the necessary human rights expertise, and involve direct, meaningful engagement with those *interested parties* (3.1.132) whose rights can be at risk.

Note 4 to entry: The analysis of the *consequences* (3.1.45) of adverse human rights impacts are measured and prioritized in terms of the severity of the impacts.

Note 5 to entry: HRRAs should be undertaken at regular intervals, recognizing that human rights risks can change over time.

Note 6 to entry: HRRAs will vary in *complexity* (3.1.43) with the size of the organization, the risk of severe human rights impacts and the nature and *context* (3.1.47) of its operations.

3.1.117
identification
process (3.1.190) of recognizing the *attributes* (3.2.5) that identify an *entity* (3.1.91)

3.1.118
impact
outcome of a *disruption* (3.1.75) affecting *objectives* (3.1.162)

3.1.119
impact analysis
consequence analysis
process (3.1.190) of analysing all operational functions and the effect that an operational interruption can have upon them

Note 1 to entry: Impact analysis is part of the *risk assessment* (3.1.219) process and includes *business impact analysis* (3.1.24). Impact analysis identifies how the loss or damage will manifest itself; the degree for potential escalation of damage or loss with time following an *incident* (3.1.122); the minimum services and *resources* (3.1.207) (human, physical, and financial) needed to enable business processes to continue to operate at a minimum acceptable level; and the timeframe and extent within which *activities* (3.1.2), functions and services of the *organization* (3.1.165) should be recovered.

3.1.120
impartiality
actual or perceived presence of objectivity

Note 1 to entry: Objectivity means that conflicts of interest do not exist or are resolved so as not to adversely influence subsequent *activities* (3.1.2).

Note 2 to entry: Other terms commonly used to convey the element of impartiality are objectivity, independence, freedom from conflict of interests, freedom from bias, lack of prejudice, neutrality, fairness, open-mindedness, even-handedness, detachment and balance.

3.1.121
improvisation
act of inventing, composing or performing, with little or no preparation, a reaction to the unexpected

3.1.122
incident
event (3.1.96) that can be, or could lead to, a *disruption* (3.1.75), loss, *emergency* (3.1.87) or *crisis* (3.1.60)

3.1.123
incident command
process (3.1.190) that is conducted as part of an *incident management system* (3.1.124), and which evolves during the *management* (3.1.144) of an *incident* (3.1.122)

3.1.124
incident management system
system that defines the roles and responsibilities of *personnel* (3.1.179) and the operating *procedures* (3.1.189) to be used in the *management* (3.1.144) of *incidents* (3.1.122)

3.1.125
incident preparedness
activities (3.1.2) taken to prepare for *incident response* (3.1.126)

3.1.126
incident response
actions taken in order to stop the causes of an imminent *hazard* (3.1.110) and/or mitigate the *consequences* (3.1.46) of potentially destabilizing *events* (3.1.96) or *disruptions* (3.1.75), and to recover to a normal situation

Note 1 to entry: Incident response is part of the *emergency management* (3.1.88) *process* (3.1.190).

3.1.127
information
data processed, organized and correlated to produce meaning

3.1.128
infrastructure
system of *facilities* (3.1.104), equipment and services needed for the operation of an *organization* (3.1.165)

[SOURCE: ISO 9000:2015, 3.5.2]

3.1.129
inherently dangerous property
property that, if in the hands of an unauthorized individual, would create an imminent *threat* (3.1.277) of death or serious bodily harm

EXAMPLE Lethal weapons, ammunition, explosives, chemical agents, biological agents and toxins, nuclear or radiological materials.

3.1.130
inject
scripted piece of *information* (3.1.127) inserted into an *exercise* (3.1.97) that is designed to elicit a response or decision and facilitate the flow of the exercise

Note 1 to entry: Injects can be written, oral, televised and/or transmitted via any means (e.g. phone, email, fax, voice, radio or sign).

3.1.131
integrity
property of safeguarding the accuracy and completeness of *assets* (3.1.13)

3.1.132
interested party
stakeholder
person or *organization* (3.1.165) that can affect, be affected by, or perceive itself to be affected by a decision or *activity* (3.1.2)

EXAMPLE Customers, *owners* (3.1.169), *personnel* (3.1.179), 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 interested parties.

Note 3 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 the example and the notes to entry.

3.1.133
internal attack
attack (3.2.4) perpetrated by people or *entities* (3.1.66) directly or indirectly linked with the legitimate manufacturer, originator of the *goods* (3.3.8) or *rights holder* (3.1.214) (staff of the rights holder, subcontractor, supplier, etc.)

3.1.134
internal audit
audit (3.1.14) conducted by, or on behalf of, an *organization* (3.1.165) itself for *management* (3.1.144) *review* (3.1.211) and other internal purposes, and which can form the basis for an organization's self-declaration of *conformity* (3.1.44)

Note 1 to entry: In many cases, particularly in smaller organizations, independence can be demonstrated by the freedom from responsibility for the *activity* (3.1.2) being audited.

3.1.135
international supply chain
supply chain (3.1.271) that at some point crosses an international or economic border

Note 1 to entry: All portions of this chain are considered international from the time a purchase order is concluded to the point where the *goods* (3.3.8) are released from customs control in the destination country or economy.

Note 2 to entry: If treaties or regional agreements have eliminated customs clearance of goods from specified countries or economies, the end of the international supply chain is the port of entry into the destination country or economy where the goods would have cleared customs if the agreements or treaties had not been in place.

3.1.136
interoperability
<diverse systems> ability of diverse systems and *organizations* (3.1.165) to work together

3.1.137
interoperability
<single-entry point> ability of single-entry point to route queries for *objects* (3.1.161) carrying *unique identifiers (UIDs)* (3.2.44) to the responsible *authoritative source* (3.2.13) for *trusted verification function (TVF)* (3.2.43)

Note 1 to entry: Interoperability includes the ability of multiple authentication systems to deliver similar responses to user groups.

[SOURCE: ISO 16678:2014, 2.1.12]

3.1.138
investment
allocation of *resources* (3.1.207) to achieve defined *objectives* (3.1.162) and other *benefits* (3.1.17)

Note 1 to entry: Investment takes two main forms: direct spending on buildings, machinery and similar *assets* (3.1.13); and indirect spending on financial securities such as bonds and shares.

[SOURCE: ISO/IEC 38500:2015, 2.13, modified — Note 1 to entry has been added.]

3.1.139
invocation
act of declaring that an *organization's* (3.1.165) *business continuity* (3.1.19) arrangements need to be put into effect in order to continue delivery of key *products or services* (3.1.158)

3.1.140
key performance indicator
KPI
quantifiable measure that an *organization* (3.1.165) uses to gauge or compare *performance* (3.1.177) in terms of meeting its strategic and operational *objectives* (3.1.162)

3.1.141
landslide
wide variety of *processes* (3.1.190) that result in the downward and outward movement of slope-forming materials including rock, soil, artificial fill or a combination of these

3.1.142
likelihood
chance of something happening

Note 1 to entry: In *risk management* (3.1.224) 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* (3.1.188) 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]

3.1.143
logical structure
arrangement of data to optimize their *access* (3.1.1) or processing by given user (human or machine)

3.1.144
management
coordinated *activities* (3.1.2) to direct and control an *organization* (3.1.165)

[SOURCE: ISO 9000:2015, 3.3.3, modified — Notes 1 and 2 to entry have been deleted.]

3.1.145
management plan
clearly defined and documented plan of action, typically covering the key *personnel* (3.1.179), *resources* (3.1.207), services, and actions needed to implement the *management* (3.1.144) *process* (3.1.190)

3.1.146
management system
set of interrelated or interacting elements of an *organization* (3.1.165) to establish *policies* (3.1.182) and *objectives* (3.1.162) and *processes* (3.1.190) 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* (3.1.180) and operation.

Note 3 to entry: The scope of a management system can 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.

Note 4 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.1.147
management system consultancy and/or associated risk assessment
participation (3.1.172) in designing, implementing or maintaining a *supply chain* (3.1.271) *security management system* (3.1.245) and in conducting *risk assessments* (3.1.219)

EXAMPLE Preparing or producing manuals or *procedures* (3.1.189); giving specific advice, instructions or solutions towards the development and implementation of a supply chain security *management system* (3.1.146); conducting *internal audits* (3.1.34); conducting risk assessment and analysis.

Note 1 to entry: Arranging *training* (3.1.280) and participating as a trainer is not considered as consultancy, provided that, where the course relates to supply chain security management systems or auditing, the course is confined to the provision of generic *information* (3.1.127) that is freely available in the public domain, i.e. the trainer does not provide company-specific solutions.

3.1.148
mass movement
displacement of materials such as soil, rock, mud, snow or a combination of matter down a slope under the influence of gravity

3.1.149
material good
manufactured, grown product or one secured from nature

3.1.150
material good life cycle
stages in the life of a *material good* (3.1.149) including conception, design, manufacture, storage, service, resell and disposal

3.1.151
maximum tolerable period of disruption
MTPD
maximum acceptable outage
MAO
time it would take for adverse *impacts* (3.1.118), which can arise as a result of not providing a product/service or performing an *activity* (3.1.2), to become unacceptable

3.1.152
measurement
process (3.1.190) to determine a value

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

3.1.153
minimum business continuity objective
MBCO
minimum *capacity* (3.1.25) or level of services and/or products that is acceptable to an *organization* (3.1.165) to achieve its business *objectives* (3.1.162) during a *disruption* (3.1.75)

3.1.154
mitigation
limitation of any negative *consequence* (3.1.46) of a particular *incident* (3.1.122)

3.1.155
monitoring
determining the status of a system, a *process* (3.1.190) or an *activity* (3.1.2)

Note 1 to entry: To determine the status, there can be a need to check, supervise or critically observe.

Note 2 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.1.156
monitoring process owner
individual or legal *entity* (3.1.91) responsible for the receipt, integration, generation, analysis, transfer and output of data

Note 1 to entry: A monitoring *process* (3.1.190) or *owner* (3.1.169) of a system within the monitoring process can be represented, e.g. by a sub-contractor.

3.1.157
mutual aid agreement
pre-arranged understanding between two or more *entities* (3.1.66) to render assistance to each other

3.1.158
nominated emergency contact
person nominated by an individual staff member who is their chosen first point of contact in the event of the *organization* (3.1.165) needing to make contact

Note 1 to entry: This can be the legal next of kin.

3.1.159
nonconformity
non-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.

3.1.160
notification
part of *public warning* (3.1.197) that provides essential *information* (3.1.127) to *people at risk* (3.1.176) regarding the decisions and actions necessary to cope with an *emergency* (3.1.87) situation

3.1.161
object
single and distinct *entity* (3.1.91) that can be identified

3.1.162
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 goals) and can apply at different levels (such as strategic, organization-wide, project, product and *process* (3.1.190)).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a *business continuity* (3.1.19) objective, or by the use of other words with similar meaning (e.g. aim, goal, or *target* (3.1.273).

Note 4 to entry: In the context of *business continuity management systems* (3.1.21), business continuity objectives are set by the *organization* (3.1.165), consistent with the business continuity *policy* (3.1.181), to achieve specific results.

Note 5 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.1.163
observer
participant (3.1.171) who witnesses the *exercise* (3.1.97) while remaining separate from exercise *activities* (3.1.2)

Note 1 to entry: Observers can be part of the *evaluation* (3.1.95) *process* (3.1.190).

3.1.164
operational information
information (3.1.127) that has been contextualized and analysed to provide an understanding of the situation and its possible evolution

3.1.165
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.1.162)

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, *partnership* (3.1.173), charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.1.166
organizational culture
collective beliefs, *values* (3.1.287), attitudes and behaviour of an *organization* (3.1.165) that contribute to the unique social and psychological environment in which it operates

3.1.167
organizational resilience
ability of an *organization* (3.1.165) to absorb and adapt in a changing environment

3.1.168
outsource
make an arrangement where an external *organization* (3.1.165) performs part of an organization's function or *process* (3.1.190)

Note 1 to entry: An external organization is outside the scope of the *management system* (3.1.146), although the outsourced function or process is within the scope.

Note 2 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.1.169
owner
entity (3.1.91) that legally controls the licensing and user rights and distribution of the *object* (3.1.161) associated with the *unique identifier (UID)* (3.2.44)

3.1.170
parameter
specific value describing the measurable or theoretical features of the elements of a system

3.1.171
participant
person or *organization* (3.1.165) who performs a function related to an *exercise* (3.1.97)

3.1.172
partnering
associating with others in an *activity* (3.1.2) or area of common interest in order to achieve individual and collective *objectives* (3.1.162)

3.1.173
partnership
organized relationship between two bodies (public–public, private–public, private–private) that establishes the scope, roles, *procedures* (3.1.189) and tools to prevent and manage any *incident* (3.1.122) impacting on *security* (3.1.239) and *resilience* (3.1.206) with respect to related laws

3.1.174
peer review
process (3.1.190) used by a *reviewer* (3.1.213) to examine the *performance* (3.1.177) of a *host* (3.1.112), provide feedback on an *analysis area* (3.1.10) and learn lessons that are transferable to its own *context* (3.1.47)

Note 1 to entry: A peer review can cover multiple analysis areas.

Note 2 to entry: The host can replace "review" with a synonym such as "assessment", "appraisal" or "analysis" to better describe the *activity* (3.1.2).

3.1.175
people aspects of business continuity
elements associated with the *management* (3.1.144) of people involved in, or affected by, an *incident* (3.1.122) in order to minimize distress, maximize productivity and *recovery* (3.1.201), and achieve the recovery *objectives* (3.1.162) of the *organization's* (3.1.165) *business continuity programme* (3.1.23)

3.1.176
people at risk
individuals in the area who could be affected by an *incident* (3.1.122)

3.1.177
performance
measurable result

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

Note 2 to entry: Performance can relate to managing *activities* (3.1.2), *processes* (3.1.190), products (including services), systems or *organizations* (3.1.165).

Note 3 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.1.178
performance evaluation
process (3.1.190) to determine measurable results against the set criteria

3.1.179
personnel
people working for and under the control of an *organization* (3.1.165)

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

3.1.180
planning
part of *management* (3.1.144) focused on setting *objectives* (3.1.162) and specifying necessary operational *processes* (3.1.190) and related *resources* (3.1.207) to fulfil the objectives

3.1.181
policy
intentions and direction of an *organization* (3.1.165), as formally expressed by its *top management* (3.1.279)

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

3.1.182
preparedness
readiness
activities (3.1.2), programmes, and systems developed and implemented prior to an *incident* (3.1.122) that can be used to support and enhance *prevention* (3.1.183), *protection* (3.1.193) from, *mitigation* (3.1.154) of, response to and *recovery* (3.1.201) from *disruptions* (3.1.75), *emergencies* (3.1.63) or *disasters* (3.1.73)

3.1.183
prevention
measures that enable an *organization* (3.1.165) to avoid, preclude or limit the *impact* (3.1.118) of an *undesirable event* (3.1.281) or potential *disruption* (3.1.75)

3.1.184
prevention of hazards and threats
process (3.1.190), practices, techniques, materials, products, services or *resources* (3.1.207) used to avoid, reduce, or control *hazards* (3.1.110) and *threats* (3.1.277) and their associated *risks* (3.1.215) of any type in order to reduce their potential *likelihood* (3.1.142) or *consequences* (3.1.46)

3.1.185
preventive action
action to eliminate the cause of a potential *nonconformity* (3.1.159) or other undesirable potential situation

Note 1 to entry: There can be more than one cause for a potential nonconformity.

Note 2 to entry: Preventive action is taken to prevent occurrence whereas *corrective action* (3.1.55) is taken to prevent recurrence.

[SOURCE: ISO 9000:2015, 3.12.1]

3.1.186
prioritized activity
activity (3.1.2) to which urgency is given in order to avoid unacceptable impacts to the business during a disruption

3.1.187
private security service provider
PSSP
private security company
PSC
organization (3.1.165) that conducts or contracts *security operations* (3.1.249) and whose business *activities* (3.1.2) include the provision of *security* (3.1.239) services either on its own behalf or on behalf of another

Note 1 to entry: PSSPs provide services to *clients* (3.1.33) with the aim of ensuring their security and that of others.

Note 2 to entry: PSSPs typically work in circumstances where governance is weak or rule of law undermined due to human- or naturally caused *events* (3.1.96) and provide services for which *personnel* (3.1.179) can be required to carry weapons in the *performance* (3.1.177) of their duties in accordance with the terms of their contract.

Note 3 to entry: Examples of security services provided by PSSPs include: guarding; close protection; physical protection measures; security awareness and *training* (3.1.280); *risk* (3.1.215), security and *threat* (3.1.277) assessment; the provision of protective and defensive measures for individuals' compounds, diplomatic and residential perimeters; escort of transport; and *policy* (3.1.181) analysis.

Note 4 to entry: A joint venture is considered part of the organization.

3.1.188
probability
measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty

Note 1 to entry: See also *likelihood* (3.1.142).

[SOURCE: ISO/Guide 73:2009, 3.6.1.4]

3.1.189
procedure
specified way to carry out an *activity* (3.1.2) or a *process* (3.1.190)

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".

3.1.190
process
set of interrelated or interacting *activities* (3.1.2) that transforms inputs into outputs

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

3.1.191
product and service
output or outcome provided by an *organization* (3.1.165) to *interested parties* (3.1.132)

EXAMPLE Manufactured items, car insurance, community nursing.

3.1.192
product fraud
wrongful or criminal deception that utilizes *material goods* (3.1.149) for financial or personal gain

Note 1 to entry: Fraud means wrongful or criminal deception intended to result in financial or personal gain that creates social or economic harm.

Note 2 to entry: Products include electronic media carried on material goods.

Note 3 to entry: Fraud related to digitally transmitted electronic media shall be considered separately.

3.1.193
protection
measures that safeguard and enable an *organization* (3.1.165) to reduce the *impact* (3.1.118) of a potential *disruption* (3.1.75)

3.1.194
psychological critical incident
event (3.1.96) or series of events that could cause significant emotional or physical distress, psychological impairment or disturbance in people's usual functioning

Note 1 to entry: Mental health professionals working in this field would normally refer to a "traumatic event" as a critical psychological incident. The term "critical psychological incident" is preferred as it implies an *incident* (3.1.122) that may or may not be traumatic to the individual involved. Although there are several definitions of a traumatic event within the psychiatric and scientific world, " psychological critical incident" provides a more real-world definition.

3.1.195
psychological education
provision of advice and guidance relating to psychological well-being

Note 1 to entry: It usually includes an overview of common reactions to distressing *events* (3.1.96) in order to normalize them, reduce anxiety, provide simple self-help strategies to facilitate recovery in the first few days, and provide advice on where and when to seek further support.

3.1.196
psychological first aid
temporary, supportive intervention comparable to the concept of physical first aid

Note 1 to entry: Its goals include stabilizing the *crisis* (3.1.60) situation, reducing emotional distress, providing advice on self-care and *psychological education* (3.1.195), identifying people who could need professional assistance and referring for further assistance, as necessary.

3.1.197
public warning
notification (3.1.160) and *alert* (3.1.6) messages disseminated as an *incident response* (3.1.126) measure to enable responders and *people at risk* (3.1.176) to take safety measures

Note 1 to entry: Public warning can include *information* (3.1.127) to raise public awareness and understanding or to provide advisory or compulsory instructions.

3.1.198
public warning system
set of protocols, *processes* (3.1.190) and technologies based on the *public warning* (3.1.197) *policy* (3.1.181) to deliver *notification* (3.1.160) and *alert* (3.1.6) messages in a developing *emergency* (3.1.87) situation to *people at risk* (3.1.176) and to first responders

3.1.199
raw material
any element, constituent or part of a *material good* (3.1.149)

3.1.200
record
document (3.1.77) stating results achieved or providing evidence of *activities* (3.1.2) performed

[SOURCE: ISO 9000:2015, 3.8.10, modified — Notes 1 and 2 to entry have been deleted.]

3.1.201
recovery
restoration and improvement, where appropriate, of operations, *facilities* (3.1.104), livelihoods or living conditions of affected *organizations* (3.1.165), including efforts to reduce *risk* (3.1.216) factors

3.1.202
recovery point objective
RPO
point to which *information* (3.1.127) used by an *activity* (3.1.2) is restored to enable the activity to operate on resumption

Note 1 to entry: Can also be referred to as "maximum data loss".

3.1.203
recovery time objective
RTO
period of time following an *incident* (3.1.122) within which a *product and service* (3.1.191) or an *activity* (3.1.2) is resumed, or *resources* (3.1.207) are recovered

Note 1 to entry: For products, services and activities, the RTO is less than the time it would take for the adverse *impacts* (3.1.118) that would arise as a result of not providing a product/service or performing an activity to become unacceptable.

3.1.204
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* (3.1.165) and *interested parties* (3.1.132) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, e.g. in *documented information* (3.1.78).

Note 3 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.1.205
residual risk
retained risk
risk (3.1.215) remaining after *risk treatment* (3.1.232)

Note 1 to entry: Residual risk can contain unidentified risk.

[SOURCE: ISO/Guide 73:2009, 3.8.1.6, modified — "retained risk" has been added as the admitted term and Note 2 to entry has been deleted.]

3.1.206
resilience
ability to absorb and adapt in a changing environment

Note 1 to entry: In the *context* (3.1.47) of *urban resilience* (3.1.284) the ability to absorb and adapt to a changing environment is determined by the collective capacity to anticipate, prepare and respond to *threats* (3.1.277) and opportunities by each individual component of an *urban system* (3.1.285).

3.1.207
resource
all assets (3.1.13) (including plant and equipment), people, skills, technology, premises, and supplies and *information* (3.1.127) (whether electronic or not) that an *organization* (3.1.165) has to have available to use, when needed, in order to operate and meet its *objective* (3.1.162)

3.1.208
response plan
documented collection of *procedures* (3.1.189) and *information* (3.1.127) that is developed, compiled and maintained in *preparedness* (3.1.182) for use in an *incident* (3.1.122)

3.1.209
response programme
plan, *processes* (3.1.190), and *resources* (3.1.207) to perform the *activities* (3.1.2) and services necessary to preserve and protect life, property, operations and critical *assets* (3.1.13)

Note 1 to entry: Response steps generally include *incident* (3.1.122) recognition, *notification* (3.1.160), assessment, declaration, plan execution, communications, and resources *management* (3.1.144).

3.1.210
response team
group of individuals responsible for developing, executing, rehearsing, and maintaining the *response plan* (3.1.208), including the *processes* (3.1.190) and *procedures* (3.1.189)

3.1.211
review
activity (3.1.2) undertaken to determine the suitability, adequacy and *effectiveness* (3.1.86) of the *management system* (3.1.146) and its component elements to achieve established *objectives* (3.1.162)

[SOURCE: ISO/Guide 73:2009, 3.8.2.2, modified — "management system and its component elements" has replaced "subject matter" and Note 1 to entry has been deleted.]

3.1.212
review visit
participation (3.1.172) by *reviewers* (3.1.213) in *peer review* (3.1.174) *activities* (3.1.2) at the *host* (3.1.112) location(s)

Note 1 to entry: Review visit activities include presentations, individual interviews, focus groups, site visits, and the observation of live and table-top *exercises* (3.1.97).

3.1.213
reviewer
entity (3.1.91) that provides feedback as part of a *peer review* (3.1.174) with expert knowledge and experience in the *analysis area* (3.1.10)

Note 1 to entry: The entity may be an *organization* (3.1.165), *partnership* (3.1.173), *community* (3.1.39), city, region, country or other body.

3.1.214
rights holder
legal *entity* (3.1.91) either holding or authorised to use one or more intellectual property rights

3.1.215
risk
effect of uncertainty on *objectives* (3.1.162)

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* (3.1.277).

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

Note 3 to entry: Risk is usually expressed in terms of *risk sources* (3.1.230), potential *events* (3.1.96), their *consequences* (3.1.45) and their *likelihood* (3.1.142).

Note 4 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards. The entry has been taken from ISO 31000:2018, 3.1, in which the words "on objectives" have been added to the definition and the notes to entry have been replaced.]

[SOURCE: ISO 31000:2018, 3.1]

3.1.216
risk acceptance
informed decision to take a particular *risk* (3.1.215)

Note 1 to entry: Risk acceptance can occur without *risk treatment* (3.1.232) or during the *process* (3.1.190) of risk treatment.

Note 2 to entry: Accepted risks are subject to *monitoring* (3.1.155) and *review* (3.1.211).

[SOURCE: ISO/Guide 73:2009, 3.7.1.6]

3.1.217
risk analysis
process (3.1.190) to comprehend the nature of *risk* (3.1.215) and to determine the level of risk

Note 1 to entry: Risk analysis provides the basis for *risk evaluation* (3.1.222) and decisions about *risk treatment* (3.1.232).

Note 2 to entry: Risk analysis includes risk estimation.

[SOURCE: ISO/Guide 73:2009, 3.6.1]

3.1.218
risk appetite
amount and type of *risk* (3.1.215) that an *organization* (3.1.165) is willing to pursue or retain

[SOURCE: ISO/Guide 73:2009, 3.7.1.2]

3.1.219
risk assessment
overall *process* (3.1.190) of *risk identification* (3.1.223), *risk analysis* (3.1.217) and *risk evaluation* (3.1.222)

Note 1 to entry: Risk assessment involves the process of identifying internal and external *threats* (3.1.277) and vulnerabilities, identifying the *likelihood* (3.1.142) and *impact* (3.1.119) of an *event* (3.1.96) arising from such threats or vulnerabilities, defining critical functions necessary to continue the *organization*'s (3.1.165) operations, defining the controls in place necessary to reduce exposure, and evaluating the cost of such controls.

Note 2 to entry: Risk assessment is described in detail in ISO 31000:2018.

[SOURCE: ISO/Guide 73:2009, 3.4.1, modified — Notes 1 and 2 to entry have been added.]

3.1.220
risk communication
exchange or sharing of *information* (3.1.127) about *risk* (3.1.215) between the decision maker and other *interested parties* (3.1.132)

Note 1 to entry: The information can relate to the existence, nature, form, *probability* (3.1.188), severity, acceptability, treatment or other aspects of risk.

3.1.221
risk criteria
terms of reference against which the significance of a *risk* (3.1.215) is evaluated

Note 1 to entry: Risk criteria are based on organizational *objectives* (3.1.162), and external and internal context.

Note 2 to entry: Risk criteria can be derived from standards, laws, *policies* (3.1.182) and other *requirements* (3.1.204).

[SOURCE: ISO/Guide 73:2009, 3.3.1.3]

3.1.222
risk evaluation
process (3.1.190) of comparing the results of *risk analysis* (3.1.217) with *risk criteria* (3.1.221) to determine whether the *risk* (3.1.215) and/or its magnitude is acceptable or tolerable

Note 1 to entry: Risk evaluation assists in the decision about *risk treatment* (3.1.232).

[SOURCE: ISO/Guide 73:2009, 3.7.1]

3.1.223
risk identification
process (3.1.190) of finding, recognizing and describing *risks* (3.1.215)

Note 1 to entry: Risk identification involves the *identification* (3.1.117) of *risk sources* (3.1.230), *events* (3.1.96), their causes and their potential *consequences* (3.1.45).

Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and *interested parties'* (3.1.132) needs.

[SOURCE: ISO/Guide 73:2009, 3.5.1, modified — In Note 2 to entry, "interested parties" has replaced "stakeholders".]

3.1.224
risk management
coordinated *activities* (3.1.2) to direct and control an *organization* (3.1.165) with regard to *risk* (3.1.215)

[SOURCE: ISO 31000:2018, 3.2]

3.1.225
risk mitigation
lessening or minimizing of the adverse *impacts* (3.1.118) of a hazardous *event* (3.1.96)

3.1.226
risk owner
entity (3.1.91) with the accountability and authority to manage a *risk* (3.1.215)

[SOURCE: ISO/Guide 73:2009, 3.5.1.5, modified — "entity" has replaced "person or entity".]

3.1.227
risk reduction
actions taken to lessen the *probability* (3.1.188) or negative *consequences* (3.1.45), or both, associated with a *risk* (3.1.215)

3.1.228
risk register
record (3.1.200) of *information* (3.1.127) about identified *risks* (3.1.215)

Note 1 to entry: Compilation for all risks identified, analysed and evaluated in the *risk assessment* (3.1.219) *process* (3.1.190), including information on the risk register includes information on *likelihood* (3.1.142), *consequences* (3.1.45), treatments and *risk owners* (3.1.226).

[SOURCE: ISO/Guide 73:2009, 3.8.2.4, modified — Note 1 to entry has been replaced.]

3.1.229
risk sharing
form of *risk treatment* (3.1.232) involving the agreed distribution of *risk* (3.1.215) with other parties

Note 1 to entry: Legal or regulatory *requirements* (3.1.204) can limit, prohibit or mandate risk sharing.

Note 2 to entry: Risk sharing can be carried out through insurance or other forms of contract.

Note 3 to entry: The extent to which risk is distributed can depend on the reliability and clarity of the sharing arrangements.

Note 4 to entry: Risk transfer is a form of risk sharing.

[SOURCE: ISO/Guide 73:2009, 3.8.1.3]

3.1.230
risk source
element that alone or in combination has the potential to give rise to *risk* (3.1.215)

[SOURCE: ISO 31000:2018, 3.4]

3.1.231
risk tolerance
organization's (3.1.165) or *interested party's* (3.1.132) readiness to bear the *risk* (3.1.215) after *risk treatment* (3.1.232) in order to achieve its *objectives* (3.1.162)

Note 1 to entry: Risk tolerance can be influenced by *client* (3.1.33), stakeholder, legal, or regulatory *requirements* (3.1.204).

[SOURCE: ISO/Guide 73:2009, 3.7.1.3, modified — "interested party" has replaced "stakeholder" and Note 1 to entry has been modified.]

3.1.232
risk treatment
process (3.1.190) to modify *risk* (3.1.215)

Note 1 to entry: Risk treatment can involve:

— avoiding the risk by deciding not to start or continue with the *activity* (3.1.2) that gives rise to the risk;

— taking or increasing risk in order to pursue an opportunity;

— removing the *risk source* (3.1.230);

— changing the *likelihood* (3.1.142);

— changing the *consequences* (3.1.45);

— sharing the risk with another party or parties (including contracts and risk financing); and

— retaining the risk by informed decision.

Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and *risk reduction* (3.1.227).

Note 3 to entry: Risk treatment can create new risks or modify existing risks.

[SOURCE: ISO/Guide 73:2009, 3.8.1]

3.1.233
robustness
ability of a system to resist virtual or physical, internal or external *attacks* (3.2.4)

Note 1 to entry: Particularly, the ability to resist attempted imitation, copy, intrusion or bypassing.

3.1.234
scenario
pre-planned storyline that drives an *exercise* (3.1.97), as well as the stimuli used to achieve exercise project *performance* (3.1.177) *objectives* (3.1.162)

3.1.235
scope of exercise
magnitude, *resources* (3.1.207) and extent that reflects the needs and *objectives* (3.1.162)

3.1.236
scope of service
function(s) that an *organization in the supply chain* (3.3.9) performs, and where it performs this/these functions

3.1.237
script
story of the *exercise* (3.1.97) as it develops, which allows directing staff to understand how *events* (3.1.96) should develop during exercise play as the various elements of the master events list are introduced

Note 1 to entry: The script is often written as a narrative of simulated events.

3.1.238
secret
data and/or knowledge that are protected against disclosure to unauthorised *entities* (3.1.66)

3.1.239
security
state of being free from danger or *threat* (3.1.277) where *procedures* (3.1.189) are followed or after taking appropriate measures

3.1.240
security aspect
characteristic, element, or property that reduces the *risk* (3.1.215) of unintentionally-, intentionally- and naturally-caused *crises* (3.1.47) and *disasters* (3.1.73) that disrupt and have *consequences* (3.1.45) on the *products and services* (3.1.158), operation, critical *assets* (3.1.13) and *continuity* (3.1.50) of an *organization* (3.1.165) and its *interested parties* (3.1.132)

3.1.241
security cleared
process (3.1.190) of verifying the trustworthiness of people who will have *access* (3.1.1) to *security sensitive information* (3.1.257)

3.1.242
security declaration
documented commitment by a *business partner* (3.3.3), which specifies *security* (3.1.239) measures implemented by that business partner, including, at a minimum, how *goods* (3.3.8) and physical instruments of international trade are safeguarded, associated *information* (3.1.127) is protected and security measures are demonstrated and verified

Note 1 to entry: It will be used by the *organization in the supply chain* (3.3.9) to evaluate the adequacy of security measures related to the security of goods.

3.1.243
security incident
any act or circumstance that produces a *consequence* (3.1.46)

3.1.244
security management
coordinated *activities* (3.1.2) to direct and control an *organization* (3.1.165) with regard to *security* (3.1.239) and *resilience* (3.1.206)

3.1.245
security management objective
specific outcome or achievement required of *security* (3.1.239) in order to meet the *security management policy* (3.1.246)

Note 1 to entry: It is essential that such outcomes are linked either directly or indirectly to providing the products, supply or services delivered by the total business to its customers or end users.

3.1.246
security management policy
overall intentions and direction of an *organization* (3.1.165), related to the *security* (3.1.239) and the framework for the control of security-related *processes* (3.1.190) and *activities* (3.1.2) that are derived from and consistent with its *policy* (3.1.181) and regulatory *requirements* (3.1.204)

3.1.247
security management programme
process (3.1.190) by which a *security management objective* (3.1.245) is achieved

3.1.248
security management target
specific level of *performance* (3.1.177) required to achieve a *security management objective* (3.1.245)

3.1.249
security operation
activity (3.1.2) and function related to the *protection* (3.1.193) of people, and tangible and intangible *assets* (3.1.13)

Note 1 to entry: *Security* (3.1.239) operations can require the carrying and operating a weapon in the *performance* (3.1.177) of their duties.

Note 2 to entry: The concept includes the International Code of Conduct (ICoC)[9] definition of security services: guarding and protection of people and *objects* (3.1.161), such as convoys, *facilities* (3.1.104), designated sites, property or other places (whether armed or unarmed) or any other activity for which the *personnel* (3.1.179) of companies are required to carry or operate a weapon in the performance of their duties.

3.1.250
security operations management
coordinated *activities* (3.1.2) to direct and control an *organization* (3.1.165) with regard to *security operations* (3.1.249)

Note 1 to entry: Direction and control with regard to security operations management generally includes establishment of the *policy* (3.1.181), *planning* (3.1.180) and *objectives* (3.1.162) directing operational *processes* (3.1.190) and *continual improvement* (3.1.49).

3.1.251
security operations objective
objective (3.1.162) sought, or aimed for, related to *security operations* (3.1.249)

Note 1 to entry: Security operations objectives are generally based on the *organization's* (3.1.165) *security operations policy* (3.1.253).

Note 2 to entry: Security operations objectives are generally specified for relevant functions and levels in the organization.

3.1.252
security operations personnel
people working on behalf of an *organization* (3.1.165) who are engaged directly or indirectly in *security operations* (3.1.249)

3.1.253
security operations policy
overall intentions and direction of an *organization* (3.1.165) related to *security operations* (3.1.249) as formally expressed by *top management* (3.1.279)

Note 1 to entry: Generally, the security operations policy is consistent with the overall *policy* (3.1.181) of the organization and provides a framework for the setting of *security operations objectives* (3.1.251).

Note 2 to entry: *Security operations management* (3.1.250) principles presented in this document can form a basis for the establishment of a security operations policy consistent with the principles and obligations outlined in the International Code of Conduct (ICoC)[9] and the Montreux Document[10].

3.1.254
security operations programme
ongoing *management* (3.1.144) and governance *process* (3.1.190) supported by *top management* (3.1.279) and resourced to ensure that the necessary steps are taken to coordinate the efforts to achieve the *objectives* (3.1.162) of the *security operations management* (3.1.250) system

3.1.255
security personnel
people in an *organization in the supply chain* (3.3.9) who have been assigned *security* (3.1.239) related duties

Note 1 to entry: These people can be employees of the *organization* (3.1.165).

3.1.256
security plan
planned arrangements for ensuring that *security* (3.1.239) is adequately managed

Note 1 to entry: It is designed to ensure the application of measures that protect the *organization* (3.1.165) from a *security incident* (3.1.243).

Note 2 to entry: The plan can be incorporated into other operational plans.

3.1.257
security sensitive information
security sensitive material
information (3.1.127) or material, produced by or incorporated into the *supply chain* (3.1.271) security *process* (3.1.190), that contains information about the *security* (3.1.239) processes, shipments or government directives that would not be readily available to the public and would be useful to someone wishing to initiate a *security incident* (3.1.243)

3.1.258
security threat scenario
means by which a potential *security incident* (3.1.243) can occur

3.1.259
self-defence
protection (3.1.193) of one's person or property against some injury attempted by another

3.1.260
sensitive information
information (3.1.127) that is protected from public disclosure only because it would have an adverse effect on an *organization* (3.1.165), national security or public safety

3.1.261
shelter in place
action to move people to predetermined areas inside the building/site in order to protect them from external dangers during an *incident* (3.1.122)

Note 1 to entry: This may be referred to as "invacuation".

3.1.262
shelter in place
remain or take immediate refuge in a protected location relevant to the *risk* (3.1.215)

3.1.263
shock
uncertain, abrupt or long-onset *event* (3.1.96), that has potential to *impact* (3.1.118) upon the purpose or *objectives* (3.1.162) of an *urban system* (3.1.285)

3.1.264
simulation
imitative representation of the functioning of one system or *process* (3.1.190) by means of the functioning of another

3.1.265
social protection
preventing, managing and overcoming situations that adversely affect people's well-being

Note 1 to entry: It consists of policies and programmes designed to reduce poverty and *vulnerability* (3.1.290) by promoting efficient labour markets, diminishing people's exposure to *risks* (3.1.215), and enhancing their *capacity* (3.1.25) to manage economic and social risks, such as unemployment, exclusion, sickness, disability and old age.

3.1.266
source
anything which alone or in combination has the intrinsic potential to give rise to *risk* (3.1.215)

Note 1 to entry: Adapted from ISO/Guide 73:2009, 3.5.1.2.

Note 2 to entry: A *risk source* (3.1.230) can be tangible or intangible.

3.1.267
spontaneous volunteer
SV
individual who is not affiliated with an existing *incident* (3.1.122) response organization or voluntary organization but who, without extensive preplanning, offers support to the response to, and *recovery* (3.1.201) from, an incident

Note 1 to entry: A spontaneous volunteer can also be referred to as a convergent volunteer, a walk-in volunteer, an occasional volunteer, an episodic volunteer or a non-affiliated volunteer.

3.1.268
strategic exercise
exercise (3.1.97) involving *top management* (3.1.279) at a strategic level

Note 1 to entry: Strategic-level top management typically includes inter-ministerial *crisis* (3.1.60) *personnel* (3.1.179), political-administrative personnel, cross-sector and cross-departmental *management* (3.1.144) personnel, and the *crisis management* (3.1.61) *organization* (3.1.165) of the corporate management team.

Note 2 to entry: Strategic exercises are designed to assess reactions to crisis in extreme situations.

Note 3 to entry: Strategic exercises are designed to develop a comprehensive *coordination* (3.1.53) and decision-making culture in organizations in the public, private and not-for-profit sectors.

3.1.269
stress
chronic and ongoing dynamic pressure originated within an *urban system* (3.1.285), with the potential for cumulative *impacts* (3.1.118) on the ability and *capacity* (3.1.25) of the system to achieve its *objectives* (3.1.162)

3.1.270
subcontracting
contracting with an external party to fulfil an obligation arising out of an existing contract

Note 1 to entry: When a party is contracted to perform a range of services, it may subcontract one or more of those services to a "subcontractor" or local forces.

Note 2 to entry: Subsidiaries of a parent company may be considered a subcontracting *organization* (3.1.165).

3.1.271
supply chain
two-way relationship of *organizations* (3.1.165), people, *processes* (3.1.190), logistics, *information* (3.1.127), technology and *resources* (3.1.207) engaged in *activities* (3.1.2) and creating value from the sourcing of materials through the delivery of *products or* services (3.1.158)

Note 1 to entry: The supply chain may include vendors, subcontractors, manufacturing *facilities* (3.1.104), logistics providers, internal distribution centres, distributors, wholesalers and other *entities* (3.1.66) that lead to the end user.

3.1.272
supply chain continuity management
SCCM
application of *business continuity management* (3.1.20) to a *supply chain* (3.1.271)

Note 1 to entry: Business continuity management should be applied to all the tiers of an *organization's* (3.1.165) supply chain.

Note 2 to entry: In practice, an organization usually would only apply it to the first tier of their suppliers and influence *critical suppliers* (3.1.68) to apply SCCM to their suppliers.

3.1.273
target
detailed *performance* (3.1.177) *requirement* (3.1.204), applicable to the *organization* (3.1.165) or parts thereof, that arises from the *objectives* (3.1.162), and that needs to be set and met in order to achieve those objectives

[SOURCE: ISO 14050:2020, 3.7.22, modified — "environmental communication" has been deleted from the term and from before "objectives" in the definition, and "or parts thereof" has been added.]

3.1.274
target group
individuals or *organizations* (3.1.165) subject to *exercise* (3.1.97)

3.1.275
test
unique and particular type of *exercise* (3.1.97), which incorporates an expectation of a pass or fail element within the aim or *objectives* (3.1.162) of the exercise being planned

Note 1 to entry: The terms "test" and *testing* (3.1.276) are not the same as "exercise" and "exercising".

3.1.276
testing
procedure (3.1.189) for *evaluation* (3.1.95), which provides a means of determining the presence, quality or veracity of something

Note 1 to entry: Testing may be referred to as a "trial".

Note 2 to entry: Testing is often applied to supporting plans.

3.1.277
threat
potential cause of an unwanted *incident* (3.1.122), which could result in harm to individuals, *assets* (3.1.13), a system or *organization* (3.1.165), the environment or the *community* (3.1.39)

3.1.278
threat analysis
process (3.1.190) of identifying, qualifying and quantifying the potential cause of an unwanted *incident* (3.1.122), which could result in harm to individuals, *assets* (3.1.13), a system or *organization* (3.1.165), the environment or the *community* (3.1.39)

3.1.279
top management
person or group of people who directs and controls an *organization* (3.1.165) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide *resources* (3.1.207) within the organization.

Note 2 to entry: If the scope of the *management system* (3.1.146) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

Note 3 to entry: This constitutes one of the common terms and core definitions of the high level structure for ISO management system standards.

3.1.280
training
activities (3.1.2) designed to facilitate the learning and development of knowledge, skills and abilities, and to improve the *performance* (3.1.177) of specific tasks or roles

3.1.281
undesirable event
occurrence or change that has the potential to cause loss of life, harm to tangible or intangible *assets* (3.1.13), or negatively *impact* (3.1.118) the *human rights* (3.1.115) and fundamental freedoms of internal or external *interested parties* (3.1.132)

3.1.282
urban agglomeration
physical structure and composition of an urban area or *continuity* (3.1.50) of large urban clusters where the built-up zone or population density of an extended city or town area or central place and any suburbs are linked by continuous, connected urban development

3.1.283
urban open area
vacant areas, public or private, within urban boundaries

Note 1 to entry: Urban open areas are all fringe open spaces and captured open spaces associated within the scope and *parameters* (3.1.170) of the *urban system* (3.1.285).

Note 2 to entry: State parks, national parks or open areas in the countryside outside the parameters of the urban area are not considered as urban open areas in this document.

3.1.284
urban resilience
ability of any *urban system* (3.1.285), with its inhabitants, in a changing environment, to anticipate, prepare, respond to and absorb *shocks* (3.1.263), positively adapt and transform in the face of *stresses* (3.1.269) and *challenges* (3.1.29), while facilitating inclusive and sustainable development

Note 1 to entry: A more resilient urban system is characterized by its ability to continue through *disruption* (3.1.75) in the short- to medium-term, combined with a *capacity* (3.1.25) to reduce pressures and adapt to changes, *risks* (3.1.215) and opportunities. Urban resilience, therefore, is dependent upon the ability of an urban systems not just to deal with shocks, but also with chronic stresses and challenges.

Note 2 to entry: Urban resilience is dependent upon the individual and collective *resilience* (3.1.206) of the separate components of a complex urban system. Although a city, town or *community* (3.1.39) within an urban area can individually demonstrate enhanced resilience within its respective boundaries, urban resilience encompasses the broader geographic scope of *urban agglomeration* (3.1.282). Resilience of an urban system is measured by the *capacity* (3.1.25) for resilience of each individual system component and dependent upon the resilience of the weakest performer among the urban agglomeration within the system scope.

Note 3 to entry: In order to assess, plan and act accordingly in the face of shocks, stresses and challenges, an urban system's capability for resilience should be measured and analysed through qualitative and quantitative data.

3.1.285
urban system
human settlement, integrated and complex set of system components, characterized by universal and interdependent dimensions: physical, functional, organizational and spatial; comprised of people, *processes* (3.1.190) and *assets* (3.1.13) managed through effective governance mechanisms

Note 1 to entry: Being dynamic, the composition and elements of an urban system changes with time.

Note 2 to entry: Every urban area has characteristics of an urban system, regardless of its size, culture, location, economy and/or political environment.

Note 3 to entry: Characterized as urban systems, urban areas have the *objectives* (3.1.162) of managing the complex interactions and interdependencies among its multiple components, with the purpose of fulfilling a variety of functionalities including social, economic, cultural and environmental.

3.1.286
use of force continuum
increasing or decreasing the level of force applied as a continuum relative to the response of the adversary, using the amount of force reasonable and necessary

Note 1 to entry: The amount of force used should be the minimum reasonable amount needed to eliminate the *threat* (3.1.277) presented, thereby minimizing the *risk* (3.1.215) and severity of any injury that can occur.

Note 2 to entry: Escalation/de-escalation of force response with a level of force should be appropriate to the situation at hand, acknowledging that the response can move from one part of the continuum to another in a matter of seconds.

3.1.287
values
beliefs an *organization* (3.1.165) adheres to and the standards that it seeks to observe

3.1.288
verification
confirmation, through the provision of objective evidence, that specified *requirements* (3.1.204) have been fulfilled

[SOURCE: ISO 9000:2015, 3.8.12, modified — Notes 1, 2 and 3 to entry have been deleted.]

3.1.289
video-surveillance
surveillance by video means

3.1.290
vulnerability
vulnerability analysis
process (3.1.190) of identifying and quantifying something that creates susceptibility to a source of *risk* (3.1.215) that can lead to a *consequence* (3.1.45)

3.1.291
vulnerability assessment
process (3.1.190) of identifying and quantifying vulnerabilities

3.1.292
vulnerable group
individuals who share one or several characteristics that are the basis of discrimination or adverse social, economic, cultural, political or health circumstances and that cause them to lack the means to achieve their rights or, otherwise, enjoy equal opportunities

3.1.293
vulnerable person
individual who might be less able to anticipate, cope with, resist or recover from the *impacts* (3.1.118) of an *emergency* (3.1.87)

Note 1 to entry: In this document, a vulnerable person is not defined by the nature of the *vulnerability* (3.1.290) but by their personal circumstances at the time of the *emergency* (3.1.87).

3.1.294
warning dissemination function
activities (3.1.2) to issue appropriate messages for *people at risk* (3.1.176) based on evidence-based *information* (3.1.127) received from the *hazard monitoring function* (3.1.111)

3.1.295
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, lighting, recognition schemes, occupational stress, ergonomics and atmospheric composition).

[SOURCE: ISO 9000:2015, 3.5.5]

3.1.296
workforce
anyone engaged in the delivery of the *organization's* (3.1.165) *objectives* (3.1.162), including direct employees, agency staff, contractors and volunteers

3.1.297
World Customs Organization
WCO
independent intergovernmental body whose mission is to enhance the *effectiveness* (3.1.86) and efficiency of customs administrations

Note 1 to entry: It is the only intergovernmental worldwide *organization* (3.1.165) competent in customs matters.

3.2 Terms related to counterfeiting tax stamps

3.2.1
activation
stage in production or use of a *tax stamp* (3.2.39) when *applicable taxes* (3.2.3) become due

Note 1 to entry: Activation of the *unique identifier (UID)* (3.2.44) used can be separate from activation of the tax stamp.

3.2.2
alteration
intentional attempt to change an authentic item or the data contained within or on an item by chemical, abrasive or other techniques

Note 1 to entry: In this document, an "item" is a *tax stamp* (3.2.39).

3.2.3
applicable tax
excise and other revenue tax on products as defined within national, state, provincial or local law

3.2.4
attack
successful or unsuccessful attempt(s) to circumvent an *authentication solution* (3.2.11), including attempts to imitate, produce or reproduce the *authentication elements* (3.2.9)

3.2.5
attribute
category of *information* (3.1.127) that comprises the content of *object* (3.1.161) *identification* (3.1.117) and authentication systems

3.2.6
attribute data management system
ADMS
system that stores, manages and controls *access* (3.1.1) of data pertaining to *objects* (3.1.161)

3.2.7
authentic material good
material good (3.1.149) produced under the control of the legitimate manufacturer, originator of the *goods* (3.3.8) or *rights holder* (3.1.214)

3.2.8
authentication
process (3.1.190) of corroborating an *entity* (3.1.91) or *attributes* (3.2.5) with a specified or understood level of assurance

Note 1 to entry: In this document, an "entity" is a *tax stamp* (3.2.39).

Note 2 to entry: The phrase "specified or understood level of assurance" acknowledges that it is impossible to achieve absolute certainty in authenticating any item. The degree of certainty varies with the type of *authentication solutions* (3.2.11) used, the *training* (3.1.280) and motivation of the examiner and the equipment available to them. For example, the level of authentication assurance achieved is very different between a consumer and a *forensic* (3.1.106) laboratory.

3.2.9
authentication element
tangible *object* (3.1.161), visual feature or *information* (3.1.127) associated with a *material good* (3.1.149) or its packaging that is used as part of an *authentication solution* (3.2.11)

3.2.10
authentication function
function performing *authentication* (3.2.8)

3.2.11
authentication solution
complete set of means and *procedures* (3.1.189) that allows the *authentication* (3.2.8) of a *material good* (3.1.149) to be performed

3.2.12
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* (3.2.9)

3.2.13
authoritative source
official origination of an *attribute* (3.2.5) that is also responsible for maintaining that attribute

3.2.14
automated interpretation
process (3.1.190) that automatically evaluates authenticity by one or more components of the *authentication solution* (3.2.11)

3.2.15
covert authentication element
authentication element (3.2.9) that is generally hidden from the human senses and can be revealed by an informed person using a tool or by *automated interpretation* (3.2.14)

3.2.16
custodian copy
duplicate that is subordinate to the *authoritative source* (3.2.13)

3.2.17
direct marking
applying a *tax stamp* (3.2.39) directly onto the product container through the use of laser marking or printing with inks or other markers that adhere to the material of the container

3.2.18
false acceptance rate
proportion of *authentications* (3.2.8) wrongly declared true

3.2.19
false rejection rate
proportion of *authentications* (3.2.8) wrongly declared false

3.2.20
forensic analysis
scientific methodology for authenticating *material goods* (3.1.149) by confirming an *authentication element* (3.2.9) or an intrinsic *attribute* (3.2.5) through the use of specialized equipment by a skilled expert with special knowledge

3.2.21
identifier
specified set of *attributes* (3.2.5) assigned to an *entity* (3.1.91) for the purpose of *identification* (3.1.117)

3.2.22
identity
set of *attributes* (3.2.5) that are related to an *entity* (3.1.91)

Note 1 to entry: An identity can have unique attributes that enable an *object* (3.1.161) to be distinguished from all others.

Note 2 to entry: Identity can be viewed in terms of human, *organization* (3.1.165) and objects (physical and intangible).

3.2.23
illicit product
taxable consumer product made available to the market to avoid the payment of all or part of the due *applicable taxes* (3.2.3)

Note 1 to entry: As part of the *risk assessment* (3.1.219), *tax authorities* (3.2.38) should refer to legislation and regulations in their jurisdictions to ascertain what qualifies as an illicit product.

Note 2 to entry: Illicit products could include illegally manufactured, adulterated, re-filled, smuggled or illegal re-imported products.

3.2.24
inspector
anyone who uses the *object examination function* (3.2.29) with the aim of evaluating an *object* (3.1.161)

[SOURCE: ISO 16678:2014, 2.1.10, modified — The notes to entry have been deleted.]

3.2.25
inspector access history
access logs detailing when *unique identifiers (UID)* (3.2.44) were checked, optionally by which (privileged) *inspector* (3.2.24) and optionally from what specific location

Note 1 to entry: Time stamps are often used.

3.2.26
integrated authentication element
authentication element (3.2.9) that is added to the *material good* (3.1.149)

3.2.27
intrinsic authentication element
authentication element (3.2.9) that is inherent to the *material good* (3.1.149)

3.2.28
lead interested party
single *interested party* (3.1.132) organizing *interoperability* (3.1.137) of *object* (3.1.161) *identification* (3.1.117) and authentication systems (I-Ps), a group of interested parties or a dedicated legal *entity* (3.1.91) governing an I-OP

3.2.29
object examination function
OEF
process (3.1.190) of finding or determining the *unique identifier (UID)* (3.2.44) or other *attributes* (3.2.5) intended to authenticate

Note 1 to entry: In this process, other attributes can assist in the *evaluation* (3.1.95) of the UID.

3.2.30
off-the-shelf authentication tool
authentication tool (3.2.12) that can be purchased through open sales networks

3.2.31
online authentication tool
authentication tool (3.2.12) that requires a real-time online connection to be able to locally interpret the *authentication element* (3.2.9)

3.2.32
overt authentication element
authentication element (3.2.9) that is detectable and verifiable by one or more of the human senses without resource to a tool (other than everyday tools that correct imperfect human senses, such as spectacles or hearing aids)

3.2.33
purpose-built authentication tool
authentication tool (3.2.12) dedicated to a specific *authentication solution* (3.2.11)

3.2.34
specifier
person or *entity* (3.1.91) who defines the *requirements* (3.1.204) for an *authentication solution* (3.2.11) to be applied to a particular *material good* (3.1.149)

3.2.35
stand-alone authentication tool
authentication tool (3.2.12) that is either used to reveal a *covert authentication element* (3.2.15) to the human senses for human *verification* (3.1.288) or that integrates the functions required to be able to verify the *authentication element* (3.2.9) independently

3.2.36
substrate
material that a *tax stamp* (3.2.39) is made of when it is produced away from the site of the *tax stamp applier* (3.2.40)

3.2.37
tamper evident
able to reveal that an item has been compromised

Note 1 to entry: In this document, an "item" refers to a *tax stamp* (3.2.39).

3.2.38
tax authority
government (national, provincial, state or local) agency that has responsibility for the collection of *applicable taxes* (3.2.3) and for the specification and design of *tax stamps* (3.2.39)

Note 1 to entry: The tax authority can be an independent agency or part of customs, the ministry of finance or other revenue authority.

3.2.39
tax stamp
visible stamp, label or mark placed on certain types of consumer *goods* (3.3.8) to show that the applicable excise tax has been paid

Note 1 to entry: It can be in the form of a label, closure seal, indicia or mark applied to the product, the package or container of the taxable item.

Note 2 to entry: Tax stamps are a tool within a government's system for the collection and *protection* (3.1.193) of *applicable taxes* (3.2.3).

Note 3 to entry: *Substrate* (3.2.36) based tax stamps are also referred to as "tax seals" and "tax banderols" (sometimes spelled "banderoles").

3.2.40
tax stamp applier
entity (3.1.91) that applies a *tax stamp* (3.2.39) to a taxable product

Note 1 to entry: The application can be done by *direct marking* (3.2.17) or by applying a *substrate* (3.2.36) based tax stamp.

Note 2 to entry: A tax stamp applier is usually a manufacturer, packager or importer of a taxable product or products, or a tax stamp supplier that is also responsible for reporting the application of the tax stamp to the *tax authority* (3.2.38), with *information* (3.1.127) about the product it is affixed to if and when required by the tax authority

3.2.41
tax stamp interested party
entity (3.1.91) with a stake in the implementation, enforcement and use of a *tax stamp* (3.2.39) system

3.2.42
trusted query processing function
TQPF
function that provides a gateway to *trusted verification function (TVF)* (3.2.43) and a*ttribute data management system (ADMS)* (3.2.6)

Note 1 to entry: This includes software running locally on a hand-held device.

3.2.43
trusted verification function
TVF
function that verifies whether a *unique identifier (UID)* (3.2.44) received is valid or not and manages a response according to rules and access privileges

3.2.44
unique identifier
UID
code that represents a single and specific set of *attributes* (3.2.5) that are related to an *object* (3.1.161) or class of objects during its life within a particular domain and scope of an object *identification* (3.1.117) system

3.3 Terms related to supply chain

3.3.1
appropriate law enforcement and other government officials
government and law enforcement *personnel* (3.1.179) that have specific legal jurisdiction over the *international supply chain* (3.1.135) or portions of it

3.3.2
authorized economic operator
party involved in the international movement of *goods* (3.3.8) in whatever function that has been approved by or on behalf of a national customs administration as conforming to relevant *supply chain* (3.1.271) security standards

Note 1 to entry: "Authorized economic operator" is a term defined in the *World Customs Organization (WCO)* (3.1.297) 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.

3.3.3
business partner
contractor, supplier or service provider with whom an *organization* (3.1.165) contracts to assist the organization in its function as an *organization in the supply chain* (3.3.9)

3.3.4
certified client
organization (3.1.165) whose *supply chain* (3.1.271) *security management* (3.1.244) system has been certified/registered by a qualified third party

3.3.5
conveyance
physical instrument of international trade that transports *goods* (3.3.8) from one location to another

EXAMPLE Box, pallet, *cargo transport unit* (3.1.27), cargo handling equipment, truck, ship, aircraft, railcar.

3.3.6
custody
period of time where an *organization in the supply chain* (3.3.9) is directly controlling the manufacturing, handling, processing and transportation of *goods* (3.3.8) and their related shipping *information* (3.1.127) within the *supply chain* (3.1.271)

3.3.7
downstream
handling, processing and movement of *goods* (3.3.8) when they are no longer in the *custody* (3.3.6) of the *organization in the supply chain* (3.3.9)

3.3.8
goods
items or materials that, upon the placement of a purchase order, are manufactured, handled, processed or transported within the *supply chain* (3.1.271) for usage or consumption by the purchaser

3.3.9
organization in the supply chain
entity (3.1.91) that:

— manufactures, handles, *processes* (3.1.190), loads, consolidates, unloads or receives *goods* (3.3.8) upon placement of a purchase order that at some point crosses an international or economy border;

— transports goods by any mode in the *international supply chain* (3.1.135) regardless of whether their particular segment of the *supply chain* (3.1.271) crosses national (or economy) boundaries; or

— provides, manages or conducts the generation, distribution or flow of shipping *information* (3.1.127) used by customs agencies or in business practices.

3.3.10
tier 1 supplier
provider of *products and services* (3.1.192) directly to an *organization* (3.1.165) usually through a contractual arrangement

3.3.11
tier 2 supplier
provider of *products and services* (3.1.192) indirectly to an *organization* (3.1.165) through a *tier 1 supplier* (3.3.10)

3.3.12
track and trace
means of identifying every individual *material good* (3.1.149) or lot(s) or batch in order to know where it is at a given time (track) and where it has been (trace) in the *supply chain* (3.1.271)

3.3.13
upstream
handling, processing and movement of *goods* (3.3.8) that occurs before the *organization in the supply chain* (3.3.9) takes *custody* (3.3.6) of the goods

3.4 Terms related to CCTV

3.4.1
dynamic metadata
data associated with a digital image aside from the pixel values, which can change for each frame of a video sequence

3.4.2
metadata
information (3.1.127) to describe audio-visual content and data essence in a format defined by ISO or any other authority

EXAMPLE Time and date, text strings, location identifying data, audio and any other associated, linked or processed information.

3.4.3
scene location
collection of *geo-locations* (3.1.109) that defines the perimeter of the viewable scene of a camera

Note 1 to entry: The coordinate system is the same for each geo-location in the collection. There is at least one geo-location in the scene location. The geo-locations are ordered in either clockwise or counter clockwise order. Single geo-location scenes interpret the geo-location as the centre of the scene.

3.4.4
semantic interoperability
ability of two or more systems or services to automatically interpret and use *information* (3.1.127) that has been exchanged accurately

3.4.5
static metadata
data associated with a digital image aside from the pixel values that does not change over time (or at least does not change over the addressed sequence)

3.4.6
syntactic interoperability
ability of two or more systems or services to exchange structured *information* (3.1.127)

Bibliography

[1] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

[2] ISO 14050:2020, *Environmental management — Vocabulary*

[3] ISO 14055-1:2017, *Environmental management — Guidelines for establishing good practices for combatting land degradation and desertification — Part 1: Good practices framework*

[4] ISO 16678:2014, *Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade*

[5] ISO 19011:2018, *Guidelines for auditing management systems*

[6] ISO 31000:2018, *Risk management — Guidelines*

[7] ISO/IEC 38500:2015, *Information technology — Governance of IT for the organization*

[8] ISO/Guide 73:2009, *Risk management — Vocabulary*

[9] ICoCA. International Code of Conduct for Private Security Service Providers. Confédération suisse, Geneva, 2010. Available at (2017-10-05): https://icoca.ch/the-code

[10] FDFA and ICRC. The Montreux Document: On pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict. Confédération suisse and International Committee of the Red Cross, Berne/ Geneva, 2008. Available at (2020-09-14): https://www.icrc.org/en/publication/0996-montreux-document-private-military-and-security-companies

Index

ICS 01.040.03; 03.100.01

Price group A