INTERNATIONAL STANDARD

ISO 22300

Second edition
2018-02

Security and resilience — Vocabulary

Sécurité et résilience — Vocabulaire

Reference number
ISO 22300:2018(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

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

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

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

Security and resilience — Vocabulary

1 Scope

This document defines terms used in security and resilience standards.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

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

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

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

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

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

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

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

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

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

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

3.5
all clear
message or signal that the danger is over

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

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

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

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

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

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

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

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

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

3.13
audit
systematic, independent and documented *process* (3.180) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: The fundamental elements of an audit include the determination of the *conformity* (3.45) of an *object* (3.151) according to a *procedure* (3.179) carried out by *personnel* (3.169) not being responsible for the object audited.

Note 2 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit or a joint audit.

Note 3 to entry: Internal audits, sometimes called first-party audits, are conducted by, or on behalf of, the *organization* (3.158) itself for *management* (3.135) *review* (3.197) and other internal purposes, and can form the basis for an organization's declaration of conformity. Independence can be demonstrated by the freedom from responsibility for the *activity* (3.1) being audited.

Note 4 to entry: External audits include those generally called second- and third-party audits. Second-party audits are conducted by parties having an interest in the organization, such as customers, or by other persons on their behalf. Third-party audits are conducted by external, independent auditing organizations such as those providing certification/registration of conformity or government agencies.

Note 5 to entry: When two or more *management systems* (3.137) are audited together, this is termed a combined audit.

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

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

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

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

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

[SOURCE: ISO 19011:2011, 3.8]

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

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

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

3.18
authentication function
function performing *authentication* (3.16)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[SOURCE: ISO/Guide 73:2009, 3.2.1, modified — In the definition, "stakeholders" has been changed to "interested parties and others" and Note 1 to entry has been modified.]

3.42
community
group of associated *organizations* (3.158), individuals and groups sharing common interests

Note 1 to entry: Impacted communities are the groups of people and associated organizations affected by the provision of *security* (3.223) services, projects or operations.

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

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

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

3.45
conformity
fulfilment of a *requirement* (3.190)

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

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

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

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

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

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

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

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

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

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

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

3.49
continuity
strategic and tactical capability, pre-approved by *management* (3.135), of an *organization* (3.158) to plan for and respond to conditions, situations and *events* (3.82) in order to continue operations at an acceptable predefined level

Note 1 to entry: Continuity is the more general term for operational and *business continuity* (3.24) to ensure an organization's ability to continue operating outside of normal operating conditions. It applies not only to for-profit companies, but to organizations of all types, such as non-governmental, public interest and governmental.

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

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

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

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

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

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

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

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

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

3.54
corrective action
action to eliminate the cause of a *nonconformity* (3.149) and to prevent recurrence

Note 1 to entry: In the case of other undesirable outcomes, action is necessary to minimize or eliminate causes and to reduce *impact* (3.107) or prevent recurrence. Such actions fall outside the concept of "corrective action" in the sense of this definition.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Note 2 to entry: Documented information can refer to:

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

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

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

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

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

3.74
drill
activity (3.1) which 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.

3.75
dynamic metadata
information (3.116) associated with a digital image aside from the pixel values that can change for each frame of a video sequence

3.76
effectiveness
extent to which planned *activities* (3.1) are realized and planned results achieved

[SOURCE: ISO 9000:2015, 3.7.11, modified — Note 1 to entry has been deleted.]

3.77
emergency
sudden, urgent, usually unexpected occurrence or *event* (3.82) requiring immediate action

Note 1 to entry: An emergency is usually a *disruption* (3.70) or condition that can often be anticipated or prepared for, but seldom exactly foreseen.

3.78
emergency management
overall approach for preventing *emergencies* (3.77) and managing those that occur

Note 1 to entry: In general, emergency management utilizes a *risk management* (3.208) approach to *prevention* (3.173), *preparedness* (3.172), response and *recovery* (3.187) before, during and after potentially destabilizing *events* (3.82) and/or *disruptions* (3.70).

3.79
entity
something that has a separate and distinct existence and that can be identified within context

Note 1 to entry: An entity can be a human, *organization* (3.158), physical *object* (3.151), class of objects or intangible object.

3.80
evacuation
organized, phased and supervised dispersal of people from dangerous or potentially dangerous areas to places of safety

3.81
evaluation
systematic *process* (3.180) that compares the result of *measurement* (3.143) to recognised criteria to determine the discrepancies between intended and actual *performance* (3.167)

Note 1 to entry: Gaps in performance are inputs into the *continual improvement* (3.48) process.

3.82
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.

Note 2 to entry: An event can consist of something not happening.

Note 3 to entry: An event can sometimes be referred to as an *incident* (3.111) or "accident".

Note 4 to entry: An event without *consequences* (3.46) can also be referred to as a "near miss", "incident", "near hit" or "close call".

Note 5 to entry: The nature, *likelihood* (3.133), and consequence of an event cannot be fully knowable.

Note 6 to entry: Likelihood associated with the event can be determined.

Note 7 to entry: An event can consist of a non-occurrence of one or more circumstances.

Note 8 to entry: An event with a consequence is sometimes referred to as an incident.

[SOURCE: ISO/Guide 73:2009, 3.5.1.3, modified — Notes 5 to 8 to entry have been added.]

3.83
exercise
process (3.180) to train for, assess, practise and improve *performance* (3.167) in an *organization* (3.158)

Note 1 to entry: Exercises can be used for validating policies, plans, *procedures* (3.179), *training* (3.265), equipment, and inter-organizational agreements; clarifying and training *personnel* (3.169) in roles and responsibilities; improving inter-organizational *coordination* (3.52) and communications; identifying gaps in *resources* (3.193); improving individual performance and identifying opportunities for improvement; and a controlled opportunity to practise improvisation.

Note 2 to entry: See also *test* (3.257).

3.84
exercise annual plan
document (3.71) in which the *exercise* (3.83) *policy* (3.171) plan has been translated to exercise goals and exercises, and in which an *exercise programme* (3.86) for a certain year is reflected

3.85
exercise coordinator
person responsible for *planning* (3.170), conducting and evaluating *exercise* (3.83) activities

Note 1 to entry: In larger exercises, this function may include several people/staff and may 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* (3.51) among internal and external entities.

3.86
exercise programme
series of *exercise* (3.83) activities designed to meet an overall *objective* (3.153) or goal

3.87
exercise programme manager
person responsible for *planning* (3.170) and improving the *exercise programme* (3.86)

3.88
exercise project team
group of individuals responsible for *planning* (3.170), conducting and evaluating an *exercise* (3.83) project

3.89
exercise safety officer
person tasked with ensuring that any actions during the *exercise* (3.83) are performed safely

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

3.90
facility
plant, machinery, property, buildings, transportation units, sea/land/air ports and other items of *infrastructure* (3.117) or plant and related systems that have a distinct and quantifiable business function or service

3.91
false acceptance rate
proportion of *authentications* (3.16) wrongly declared true

3.92
false rejection rate
proportion of *authentications* (3.16) wrongly declared false

3.93
forensic
related to, or used in, courts of law

Note 1 to entry: This applies to video-surveillance used to produce legal evidence.

3.94
forensic analysis
scientific methodology for authenticating *material goods* (3.139) by confirming an *authentication element* (3.17) or an intrinsic attribute through the use of specialized equipment by a skilled expert with special knowledge

3.95
full-scale exercise
exercise (3.83) which involves multiple *organizations* (3.158) or functions and includes actual *activities* (3.1)

3.96
functional exercise
exercise (3.83) to train for, assess, practise and improve the *performance* (3.167) of single functions designed to respond to and recover from an unwanted *event* (3.82)

Note 1 to entry: Functions can include an emergency operations centre (EOC) team, a *crisis management team* (3.61) or fire-fighters decontaminating mock victims.

3.97
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* (3.151) on the earth. The term itself does not carry a prescription of the coordinate system to be used. Additional attributes associated with a geo-location are not a part of a geo-location specification.

3.98
goods
items or materials that, upon the placement of a purchase order, are manufactured, handled, processed or transported within the *supply chain* (3.251) for usage or consumption by the purchaser

3.99
hazard
source of potential harm

Note 1 to entry: Hazard can be a *risk source* (3.213).

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

3.100
hazard monitoring function
activities (3.1) to obtain evidence-based *information* (3.116) on *hazards* (3.99) in a defined area used to make decisions about the need for *public warning* (3.183)

3.101
hue
attribute 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

3.102
human interpretation
authenticity as evaluated by an *inspector* (3.120)

3.103
human rights risk analysis
HRRA
process (3.180) to identify, analyse, evaluate and document human rights-related *risks* (3.199) and their *impacts* (3.107), in order to manage risk and to mitigate or prevent adverse human rights impacts and legal infractions

Note 1 to entry: The HRRA is part of the *organization's* (3.158) *requirement* (3.190) 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* (3.203).

Note 3 to entry: The HRRA includes an analysis of the severity of actual and potential human rights impacts that the organization may cause or contribute to through its *security operations* (3.232), or which may 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* (3.124) whose rights may be at risk.

Note 4 to entry: The analysis of the *consequences* (3.46) 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 may change over time.

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

Note 7 to entry: HRRA is sometimes referred to as a "human rights risk assessment", a "human rights impact assessment" or a "human rights risk and impact assessment".

3.104
identification
process (3.180) of recognizing the attributes that identify an *entity* (3.79)

3.105
identifier
specified set of attributes assigned to an *entity* (3.79) for the purpose of *identification* (3.104)

3.106
identity
set of attributes that are related to an *entity* (3.79)

Note 1 to entry: An identity can have unique attributes that enable an *object* (3.151) to be distinguished from all others.

Note 2 to entry: Identity can be viewed in terms of human, *organization* (3.158) and objects (physical and intangible).

3.107
impact
evaluated *consequence* (3.46) of a particular outcome

3.108
impact analysis
consequence analysis
process (3.180) 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* (3.203) process and includes *business impact analysis* (3.29). 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* (3.111); the minimum services and resources (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), functions and services of the organization should be recovered.

3.109
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.

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.

3.110
improvisation
act of inventing, composing or performing, with little or no preparation, a reaction to the unexpected

3.111
incident
situation that can be, or could lead to, a *disruption* (3.70), loss, *emergency* (3.77) or *crisis* (3.59)

3.112
incident command
process that is conducted as part of an incident *management system* (3.137), and which evolves during the *management* (3.135) of an *incident* (3.111)

3.113
incident management system
system that defines the roles and responsibilities of *personnel* (3.169) and the operating *procedures* (3.179) to be used in the management of incidents

3.114
incident preparedness
activities (3.1) taken to prepare for *incident response* (3.115)

3.115
incident response
actions taken in order to stop the causes of an imminent *hazard* (3.99) and/or mitigate the *consequences* (3.46) of potentially destabilizing *events* (3.82) or *disruptions* (3.70), and to recover to a normal situation

Note 1 to entry: Incident response is part of the *emergency management* (3.78) *process* (3.180).

3.116
information
data processed, organized and correlated to produce meaning

3.117
infrastructure
system of *facilities* (3.90), equipment and services needed for the operation of an *organization* (3.158)

[SOURCE: ISO 9000:2015, 3.5.2]

3.118
inherently dangerous property
property that, if in the hands of an unauthorized individual, would create an imminent *threat* (3.259) of death or serious bodily harm

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

3.119
inject
scripted piece of *information* (3.116) inserted into an *exercise* (3.83) 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).

3.120
inspector
person who uses the *object examination function* (3.152) with the aim of evaluating an *object* (3.151)

Note 1 to entry: Any *participant* (3.163) within an identification and authentication system can act as an inspector.

Note 2 to entry: Inspectors can have different levels of qualification and *training* (3.265).

Note 3 to entry: The inspector can be an automated system.

3.121
inspector access history
access logs detailing when *unique identifiers* (UID) (3.269) were checked, optionally by which (privileged) *inspector* (3.120), and optionally from what specific location

Note 1 to entry: Time stamps are often used.

3.122
integrated authentication element
authentication element (3.17) that is added to the *material good* (3.139)

3.123
integrity
property of safeguarding the accuracy and completeness of *assets* (3.10)

3.124
interested party
stakeholder
person or *organization* (3.158) that can affect, be affected by, or perceive itself to be affected by a decision or *activity* (3.1)

EXAMPLE Customers, *owners* (3.162), people in an organization, 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 external interested parties.

Note 3 to entry: Throughout this document, the use of the term "interested party" is consistent with its usage in *security operations* (3.232).

[SOURCE: ISO 9000:2015, 3.2.3, modified — Note 1 to entry has been replaced and Notes 2 and 3 to entry have been added.]

3.125
internal attack
attack (3.11) perpetrated by people or entities directly or indirectly linked with the legitimate manufacturer, originator of the *goods* (3.98) or *rights holder* (3.198) (staff of the rights holder, subcontractor, supplier, etc.)

3.126
internal audit
audit (3.13) conducted by, or on behalf of, an *organization* (3.158) itself for *management* (3.135) *review* (3.197) and other internal purposes, and which can form the basis for an organization's self-declaration of *conformity* (3.45)

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) being audited.

3.127
international supply chain
supply chain (3.251) 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* (3.98) 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.

3.128
interoperability
ability of diverse systems and *organizations* (3.158) to work together

3.129
intrinsic authentication element
authentication element (3.17) which is inherent to the *material good* (3.139)

3.130
invocation
act of declaring that an *organization's* (3.158) *business continuity* (3.24) arrangements need to be put into effect in order to continue delivery of key *products or services* (3.181)

3.131
key performance indicator
KPI
quantifiable measure that an *organization* (3.158) uses to gauge or compare *performance* (3.167) in terms of meeting its strategic and operational *objectives* (3.153)

3.132
less-lethal force
degree of force used that is less likely to cause death or serious injury to overcome violent encounters and appropriately meet the levels of resistance encountered

3.133
likelihood
chance of something happening

Note 1 to entry: In *risk management* (3.208) 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* (3.178) 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/Guide 73:2009, 3.6.1.1]

3.134
logical structure
arrangement of data to optimize their access or processing by given user (human or machine)

3.135
management
coordinated *activities* (3.1) to direct and control an *organization* (3.158)

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

3.136
management plan
clearly defined and documented plan of action, typically covering the key *personnel* (3.169), *resources* (3.193), services, and actions needed to implement the *management* (3.135) *process* (3.180)

3.137
management system
set of interrelated or interacting elements of an *organization* (3.158) to establish policies and *objectives* (3.153), and *processes* (3.180) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines, e.g. quality management, financial management or environmental management.

Note 2 to entry: The management system elements establish the organization's structure, roles and responsibilities, *planning* (3.170), operation, policies, practices, rules, beliefs, objectives and processes to achieve those objectives.

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.

[SOURCE: ISO 9000:2015, 3.5.3, modified — Note 4 to entry has been deleted.]

3.138
management system consultancy and/or associated risk assessment
participation in designing, implementing or maintaining a *supply chain* (3.251) *security management* (3.227) system and in conducting *risk assessments* (3.203)

EXAMPLE preparing or producing manuals or *procedures* (3.179); giving specific advice, instructions or solutions towards the development and implementation of a supply chain security management system; conducting *internal audits* (3.126); conducting risk assessment and analysis.

Note 1 to entry: Arranging *training* (3.265) 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* (3.116) that is freely available in the public domain, i.e. the trainer does not provide company-specific solutions.

3.139
material good
manufactured, grown product or one secured from nature

3.140
material good life cycle
stages in the life of a *material good* (3.139) including conception, design, manufacture, storage, service, resell and disposal

3.141
maximum acceptable outage
MAO
time it would take for adverse *impacts* (3.107), which can arise as a result of not providing a product/service or performing an *activity* (3.1), to become unacceptable

Note 1 to entry: See also *maximum tolerable period of disruption* (3.142).

3.142
maximum tolerable period of disruption
MTPD
time it would take for adverse *impacts* (3.107), which can arise as a result of not providing a product/service or performing an *activity* (3.1), to become unacceptable

Note 1 to entry: See also *maximum acceptable outage* (3.141).

3.143
measurement
process (3.180) to determine a value

[SOURCE: ISO 9000:2015, 3.11.4, modified — Notes 1 and 2 to entry have been deleted.]

3.144
metadata
information (3.116) to describe audiovisual content and data essence in a defined format

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

3.145
minimum business continuity objective
MBCO
minimum level of services and/or products that is acceptable to an *organization* (3.158) to achieve its business *objectives* (3.153) during a *disruption* (3.70)

3.146
mitigation
limitation of any negative *consequence* (3.46) of a particular *incident* (3.111)

3.147
monitoring
determining the status of a system, a *process* (3.180), a product, a service, or an *activity* (3.1)

Note 1 to entry: For the determination of the status, there can be a need to check, supervise or critically observe.

[SOURCE: ISO 9000:2015, 3.11.3, modified — Notes 2 and 3 to entry have been deleted.]

3.148
mutual aid agreement
pre-arranged understanding between two or more entities to render assistance to each other

3.149
nonconformity
non-fulfilment of a *requirement* (3.190)

[SOURCE: ISO 9000:2015, 3.6.9, modified — Note 1 to entry has been deleted.]

3.150
notification
part of *public warning* (3.183) that provides essential *information* (3.116) to *people at risk* (3.166) regarding the decisions and actions necessary to cope with an *emergency* (3.77) situation

3.151
object
single and distinct *entity* (3.79) that can be identified

3.152
object examination function
OEF
process (3.180) of finding or determining the *unique identifier (UID)* (3.269) or other attributes intended to authenticate

Note 1 to entry: In this process, other attributes can assist in the *evaluation* (3.81) of the UID.

3.153
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 objectives) and can apply at different levels (such as strategic, organization-wide, project, product and *process* (3.180)).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion or by the use of other words with similar meaning (e.g. aim, goal, or *target* (3.255)).

Note 4 to entry: In the context of *security operations management* (3.233) systems, *security operations objectives* (3.234) are set by the organization, consistent with the *security operations policy* (3.236), to achieve specific results.

[SOURCE: ISO 9000:2015, 3.7.1, modified — In Note 4 to entry, "security operations management systems" has replaced "quality management systems" and Note 5 to entry has been deleted.]

3.154
observer
participant (3.163) who witnesses the *exercise* (3.83) while remaining separate from exercise activities

Note 1 to entry: Observers may be part of the *evaluation* (3.81) *process* (3.180).

3.155
off-the-shelf authentication tool
authentication tool (3.20) that can be purchased through open sales networks

3.156
on-line authentication tool
authentication tool (3.20) that requires a real-time on-line connection to be able to locally interpret the *authentication element* (3.17)

3.157
operational information
information (3.116) that has been contextualized and analysed to provide an understanding of the situation and its possible evolution

3.158
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.153)

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, *partnership* (3.165), charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: For organizations with more than one operating unit, a single operating unit can be defined as an organization.

[SOURCE: ISO 9000:2015, 3.2.1, modified — Note 2 to entry has been replaced.]

3.159
organization in the supply chain
entity (3.79) that

— manufactures, handles, processes, loads, consolidates, unloads or receives *goods* (3.98) 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* (3.127) regardless of whether their particular segment of the *supply chain* (3.251) crosses national (or economy) boundaries, or

— provides, manages or conducts the generation, distribution or flow of shipping *information* (3.116) used by customs agencies or in business practices.

3.160
outsource
make an arrangement where an external *organization* (3.158) performs part of an organization's function or *process* (3.180)

Note 1 to entry: An external organization is outside the scope of the *management system* (3.137), although the outsourced function or process is within the scope.

[SOURCE: ISO 9000:2015, 3.4.6, modified — Note 2 to entry has been deleted.]

3.161
overt authentication element
authentication element (3.17) that is detectable and verifiable by one or more of the human senses without resource to a tool (other than everyday tools which correct imperfect human senses, such as spectacles or hearing aids)

3.162
owner
entity (3.79) that legally controls the licensing and user rights and distribution of the *object* (3.151) associated with the *unique identifier (UID)* (3.269)

3.163
participant
person or *organization* (3.158) who performs a function related to an *exercise* (3.83)

3.164
partnering
associating with others in an *activity* (3.1) or area of common interest in order to achieve individual and collective *objectives* (3.153)

3.165
partnership
organized relationship between two bodies (public–public, private–public, private–private) which establishes the scope, roles, *procedures* (3.179) and tools to prevent and manage any *incident* (3.111) impacting on *security* (3.223) and *resilience* (3.192) with respect to related laws

3.166
people at risk
individuals in the area who may be affected by an *incident* (3.111)

3.167
performance
measurable result

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

Note 2 to entry: Performance can relate to the *management* (3.135) of *activities* (3.1), *processes* (3.180), products, services, systems or *organizations* (3.158).

[SOURCE: ISO 9000:2015, 3.7.8, modified — Note 3 to entry has been deleted.]

3.168
performance evaluation
process (3.180) of determining measurable results

3.169
personnel
people working for and under the control of an *organization* (3.158)

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

3.170
planning
part of *management* (3.135) focused on setting *security operations objectives* (3.234) and specifying necessary operational *processes* (3.180) and related *resources* (3.193) to fulfil the security operations objectives

3.171
policy
intentions and direction of an *organization* (3.158) as formally expressed by its *top management* (3.263)

[SOURCE: ISO 9000:2015, 3.5.8, modified — Note 1 to entry has been deleted.]

3.172
preparedness
readiness
activities (3.1), programmes, and systems developed and implemented prior to an *incident* (3.111) that can be used to support and enhance prevention, protection from, mitigation of, response to and recovery from *disruptions* (3.70), *emergencies* (3.77) or *disasters* (3.69)

3.173
prevention
measures that enable an *organization* (3.158) to avoid, preclude or limit the *impact* (3.107) of an *undesirable event* (3.268) or potential *disruption* (3.70)

3.174
prevention of hazards and threats
process (3.180), practices, techniques, materials, products, services or *resources* (3.193) used to avoid, reduce, or control *hazards* (3.99) and *threats* (3.259) and their associated *risks* (3.199) of any type in order to reduce their potential *likelihood* (3.133) or *consequences* (3.46)

3.175
preventive action
action to eliminate the cause of a potential *nonconformity* (3.149) 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* (3.54) is taken to prevent recurrence.

[SOURCE: ISO 9000:2015, 3.12.1]

3.176
prioritized activity
activity (3.1) to which priority is given following an *incident* (3.111) in order to mitigate *impacts* (3.107)

Note 1 to entry: Terms commonly used to describe these activities include critical, essential, vital, urgent and key.

3.177
private security service provider
private security company
PSC
organization (3.158) that conducts or contracts *security operations* (3.232) and whose business activities include the provision of *security* (3.223) services either on its own behalf or on behalf of another

Note 1 to entry: PSCs provide services to *clients* (3.35) with the aim of ensuring their security and that of others.

Note 2 to entry: PSCs typically work in circumstances where governance is weak or rule of law undermined due to human- or naturally-caused *events* (3.82) and provide services for which *personnel* (3.169) can be required to carry weapons in the *performance* (3.167) of their duties in accordance with the terms of their contract.

Note 3 to entry: Examples of security services provided by PSCs include: guarding; close protection; physical protection measures; security awareness and *training* (3.265); *risk* (3.199), security and threat assessment; the provision of protective and defensive measures for individuals compounds, diplomatic and residential perimeters; escort of transport; and *policy* (3.171) analysis.

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

3.178
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* (3.133).

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

3.179
procedure
specified way to carry out an *activity* (3.1) or a *process* (3.180)

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".

3.180
process
set of interrelated or interacting *activities* (3.1) that use inputs to deliver an intended result

[SOURCE: ISO 9000:2015, 3.4.1, modified — Notes 1 to 6 to entry have been deleted.]

3.181
product or service
beneficial outcome provided by an *organization* (3.158) to its customers, recipients and *interested parties* (3.124)

EXAMPLE Manufactured items, car insurance, community nursing.

3.182
protection
measures that safeguard and enable an *organization* (3.158) to reduce the *impact* (3.107) of a potential *disruption* (3.70)

3.183
public warning
notification (3.150) and *alert* (3.4) messages disseminated as an *incident response* (3.115) measure to enable responders and *people at risk* (3.166) to take safety measures

Note 1 to entry: Public warning can include *information* (3.116) to raise public awareness and understanding or to provide advisory or compulsory instructions.

3.184
public warning system
set of protocols, *processes* (3.180) and technologies based on the *public warning* (3.183) *policy* (3.171) to deliver *notification* (3.150) and *alert* (3.4) messages in a developing *emergency* (3.77) situation to *people at risk* (3.166) and to first responders

3.185
purpose-built authentication tool
authentication tool (3.20) dedicated to a specific *authentication solution* (3.19)

3.186
record
document (3.71) stating results achieved or providing evidence of *activities* (3.1) performed

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

3.187
recovery
restoration and improvement, where appropriate, of operations, *facilities* (3.90), livelihoods or living conditions of affected *organizations* (3.158), including efforts to reduce *risk* (3.199) factors

3.188
recovery point objective
RPO
point to which *information* (3.116) used by an *activity* (3.1) is restored to enable the activity to operate on resumption

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

3.189
recovery time objective
RTO
period of time following an *incident* (3.111) within which a *product or service* (3.181) or an *activity* (3.1) is resumed, or *resources* (3.193) are recovered

Note 1 to entry: For products, services and activities, the recovery time objective is less than the time it would take for the adverse *impacts* (3.107) that would arise as a result of not providing a product/service or performing an activity to become unacceptable.

3.190
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* (3.158) and *interested parties* (3.124) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, for example in documented *information* (3.116).

[SOURCE: ISO 9000:2015, 3.6.4, modified — Notes 3 to 6 to entry have been deleted.]

3.191
residual risk
risk (3.199) remaining after *risk treatment* (3.215)

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

Note 2 to entry: Residual risk can also be known as "retained risk".

[SOURCE: ISO/Guide 73:2009, 3.8.1.6]

3.192
resilience
ability to absorb and adapt in a changing environment

3.193
resource
asset, *facility* (3.90), equipment, material, product or waste that has potential value and can be used

3.194
response plan
documented collection of *procedures* (3.179) and *information* (3.116) that is developed, compiled and maintained in readiness for use in an *incident* (3.111)

3.195
response programme
plan, *processes* (3.180), and *resources* (3.193) to perform the *activities* (3.1) and services necessary to preserve and protect life, property, operations and critical *assets* (3.10)

Note 1 to entry: Response steps generally include *incident* (3.111) recognition, *notification* (3.150), assessment, declaration, plan execution, communications, and resources *management* (3.135).

3.196
response team
group of individuals responsible for developing, executing, rehearsing, and maintaining the *response plan* (3.194), including the *processes* (3.180) and *procedures* (3.179)

3.197
review
activity (3.1) undertaken to determine the suitability, adequacy and *effectiveness* (3.76) of the *management system* (3.137) and its component elements to achieve established *objectives* (3.153)

[SOURCE: ISO/Guide 73:2009, 3.8.2.2, modified — Note 1 to entry has been deleted.]

3.198
rights holder
legal *entity* (3.79) either holding or authorised to use one or more intellectual property rights

3.199
risk
effect of uncertainty on *objectives* (3.153)

Note 1 to entry: An effect is a deviation from the expected — positive and/or negative.

Note 2 to entry: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

Note 3 to entry: Risk is often characterized by reference to potential events and *consequences* (3.46), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

[SOURCE: ISO/Guide 73:2009, 1.1]

3.200
risk acceptance
informed decision to take a particular *risk* (3.199)

Note 1 to entry: Risk acceptance can occur without *risk treatment* (3.215) or during the *process* (3.180) of risk treatment.

Note 2 to entry: Accepted risks are subject to *monitoring* (3.147) and *review* (3.197).

[SOURCE: ISO/Guide 73:2009, 3.7.1.6, modified — Note 5 to entry has been added.]

3.201
risk analysis
process (3.180) to comprehend the nature of *risk* (3.199) and to determine the level of risk

Note 1 to entry: Risk analysis provides the basis for *risk evaluation* (3.206) and decisions about *risk treatment* (3.215).

Note 2 to entry: Risk analysis includes risk estimation.

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

3.202
risk appetite
amount and type of *risk* (3.199) that an *organization* (3.158) is willing to pursue or retain

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

3.203
risk assessment
overall *process* (3.180) of *risk identification* (3.207), *risk analysis* (3.201) and *risk evaluation* (3.206)

Note 1 to entry: Risk assessment involves the process of identifying internal and external *threats* (3.259) and vulnerabilities, identifying the *likelihood* (3.133) and *impact* (3.107) of an *event* (3.82) arising from such threats or vulnerabilities, defining critical functions necessary to continue the *organization*'s (3.158) operations, defining the controls in place necessary to reduce exposure, and evaluating the cost of such controls.

[SOURCE: ISO/Guide 73:2009, 3.4.1, modified — Note 1 to entry has been added.]

3.204
risk communication
exchange or sharing of *information* (3.116) about *risk* (3.199) between the decision maker and other *interested parties* (3.124)

Note 1 to entry: The information can relate to the existence, nature, form, *probability* (3.178), severity, acceptability, treatment or other aspects of risk.

3.205
risk criteria
terms of reference against which the significance of a *risk* (3.199) is evaluated

Note 1 to entry: Risk criteria are based on organizational *objectives* (3.153), and external and internal context.

Note 2 to entry: Risk criteria can be derived from standards, laws, policies and other *requirements* (3.190).

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

3.206
risk evaluation
process (3.180) of comparing the results of *risk analysis* (3.201) with *risk criteria* (3.205) to determine whether the *risk* (3.199) and/or its magnitude is acceptable or tolerable

Note 1 to entry: Risk evaluation assists in the decision about *risk treatment* (3.215).

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

3.207
risk identification
process (3.180) of finding, recognizing and describing *risks* (3.199)

Note 1 to entry: Risk identification involves the *identification* (3.104) of *risk sources* (3.213), *events* (3.82), their causes and their potential *consequences* (3.46).

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

[SOURCE: ISO/Guide 73:2009, 3.4.1, modified — In Note 2 to entry, "stakeholders'" has been changed to "interested parties'".]

3.208
risk management
coordinated *activities* (3.1) to direct and control an *organization* (3.158) with regard to *risk* (3.199)

Note 1 to entry: Risk management generally includes *risk assessment* (3.203), *risk treatment* (3.215), *risk acceptance* (3.200), and *risk communication* (3.204).

[SOURCE: ISO/Guide 73:2009, 2.1, modified — Note 1 to entry has been added.]

3.209
risk owner
entity (3.79) with the accountability and authority to manage a *risk* (3.199)

[SOURCE: ISO/Guide 73:2009, 3.4.5]

3.210
risk reduction
actions taken to lessen the *probability* (3.178) or negative *consequences* (3.46), or both, associated with a *risk* (3.199)

3.211
risk register
record (3.186) of *information* (3.116) about identified *risks* (3.199)

Note 1 to entry: Compilation for all risks identified, analysed and evaluated in the *risk assessment* (3.203) *process* (3.180), including information on the risk register includes information on *likelihood* (3.133), *consequences* (3.46), treatments and *risk owners* (3.209).

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

3.212
risk sharing
form of *risk treatment* (3.215) involving the agreed distribution of *risk* (3.199) with other parties

Note 1 to entry: Legal or regulatory *requirements* (3.190) 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]

3.213
risk source
element which alone or in combination has the intrinsic potential to give rise to *risk* (3.199)

Note 1 to entry: A risk source can be tangible or intangible.

[SOURCE: ISO/Guide 73:2009, 3.5.1.2]

3.214
risk tolerance
organization's (3.158) or interested party's readiness to bear the *risk* (3.199) after *risk treatment* (3.215) in order to achieve its *objectives* (3.153)

Note 1 to entry: Risk tolerance can be influenced by *client* (3.35), stakeholder, legal, or regulatory *requirements* (3.190).

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

3.215
risk treatment
process (3.180) to modify *risk* (3.199)

Note 1 to entry: Risk treatment can involve

— avoiding the risk by deciding not to start or continue with the *activity* (3.1) that gives rise to the risk,

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

— removing the *risk source* (3.213),

— changing the *likelihood* (3.133),

— changing the *consequences* (3.46),

— 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* (3.210)".

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

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

3.216
robustness
ability of a system to resist virtual or physical, internal or external *attacks* (3.11)

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

3.217
scenario
pre-planned storyline that drives an *exercise* (3.83), as well as the stimuli used to achieve exercise project *performance* (3.167) *objectives* (3.153)

3.218
scene location
collection of *geo-locations* (3.97) that define 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.

3.219
scope of exercise
magnitude, *resources* (3.193) and extent which reflects the needs and *objectives* (3.153)

3.220
scope of service
function(s) that an *organization in the supply chain* (3.159) performs, and where it performs this/these functions

3.221
script
story of the *exercise* (3.83) as it develops which allows directing staff to understand how *events* (3.82) 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.

3.222
secret
data and/or knowledge that are protected against disclosure to unauthorised entities

3.223
security
state of being free from danger or *threat* (3.259)

3.224
security aspect
characteristic, element, or property that reduces the *risk* (3.199) of unintentionally-, intentionally-, and naturally-caused *crises* (3.59) and *disasters* (3.69) which disrupt and have *consequences* (3.46) on the *products or services* (3.181), operation, critical *assets* (3.10) and *continuity* (3.49) of an *organization* (3.158) and its *interested parties* (3.124)

3.225
security cleared
process (3.180) of verifying the trustworthiness of people who will have access to *security sensitive information* (3.240)

3.226
security declaration
documented commitment by a *business partner* (3.30), which specifies *security* (3.223) measures implemented by that business partner, including, at a minimum, how *goods* (3.98) and physical instruments of international trade are safeguarded, associated *information* (3.116) is protected and security measures are demonstrated and verified

Note 1 to entry: It will be used by the *organization in the supply chain* (3.159) to evaluate the adequacy of security measures related to the security of goods.

3.227
security management
systematic and coordinated *activities* (3.1) and practices through which an *organization* (3.158) optimally manages its *risks* (3.199), and the associated potential *threats* (3.259) and *impacts* (3.107)

3.228
security management objective
specific outcome or achievement required of *security* (3.223) in order to meet the *security management policy* (3.229)

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.

3.229
security management policy
overall intentions and direction of an *organization* (3.158), related to the *security* (3.223) and the framework for the control of security-related *processes* (3.180) and *activities* (3.1) that are derived from and consistent with its *policy* (3.171) and regulatory *requirements* (3.190)