Practical Project Management

DRAFT – DRAFT – DRAFT

H.T.G. Weffers ● 29 December 2020

Glossary

To be able to work effectively and efficiently and to avoid miscommunication, people who engage in a joint endeavour need to have a common reference with respect to the terminology they will use in that endeavour. Given the nature of our joint endeavour, we chose to use the following set of internationally recognized standards [1, 2, 3] as the basis of our common reference:

- ISO 9000:2015 *Quality management systems — Fundamentals and vocabulary*
- ISO 10005:2018 *Quality management — Guidelines for quality plans*
- ISO 10006:2017 *Quality management — Guidelines for quality management in projects*
- ISO 10007:2017 *Quality management — Guidelines for configuration management*
- ISO Guide 73:2009 *Risk management — Vocabulary*
- ISO 31000:2018 *Risk management — Guidelines*
- ISO 21500 *Project, programme and portfolio management — Context and concepts*
- ISO 21502 *Project, programme and portfolio management — Guidance on project management*
- ISO 21503:2017 *Project, programme and portfolio management — Guidance on programme management*
- ISO 21504:2015 *Project, programme and portfolio management — Guidance on portfolio management*
- ISO 21505:2017 *Project, programme and portfolio management — Guidance on governance*
- ISO/TR 21506:2018 *Project, programme and portfolio management — Vocabulary*
- ISO 26000:2010 *Guidance on social responsibility*
- ISO/IEC Guide 51:2014 *Safety aspects — Guidelines for their inclusion in standards*
- ISO 22300:2018 *Security and resilience — Vocabulary*
- ISO/IEC 2382:2015 *Information technology — Vocabulary*
- ISO/IEC 20546:2019 *Information technology — Big data — Overview and vocabulary*
- ISO/IEC 17788:2014 *Information technology — Cloud computing — Overview and vocabulary*
- ISO/IEC 20924:2018 *Information technology — Internet of Things (IoT) — Vocabulary*
- ISO/IEC/IEEE 15288:2015 *Systems and software engineering — System life cycle processes*
- ISO/IEC/IEEE 12207:2017 *Systems and software engineering — Software life cycle processes*
- ISO/IEC/IEEE 26515:2018 *Systems and software engineering — Developing information for users in an agile environment*
- ISO/IEC TR 24774:2010 *Systems and software engineering — Life cycle management — Guidelines for process description*
- ISO/IEC/IEEE 16085 *Systems and software engineering — Life cycle processes — Risk management*
- ISO/IEC/IEEE 16326:2019 *Systems and software engineering — Life cycle processes — Project management*
- ISO/IEC/IEEE 29148:2018 *Systems and software engineering — Life cycle processes — Requirements engineering*
- ISO/IEC/IEEE 24748-1:2018 *Systems and software engineering — Life cycle management — Part 1: Guidelines for life cycle management*
- ISO/IEC/IEEE 24748-4:2016 *Systems and software engineering — Life cycle management — Part 4: Systems engineering planning*
- ISO/IEC/IEEE 24748-5:2017 *Systems and software engineering — Life cycle management — Part 5: Software development planning*
- ISO/IEC/IEEE 29119-1:2013 *Software and systems engineering — Software testing — Part 1: Concepts and definitions*
- ISO/IEC/IEEE 15939:2017 *Systems and software engineering — Measurement process*
- ISO/IEC/IEEE 42010:2011 *Systems and software engineering — Architecture description*
- ISO/IEC/IEEE DIS 42010 *Software, systems and enterprise — Architecture description*
- ISO/IEC/IEEE 42020:2019 *Software, systems and enterprise — Architecture processes*
- ISO/IEC/IEEE 42030:2019 *Software, systems and enterprise — Architecture evaluation framework*
- ISO/IEC 20246:2017 *Software and systems engineering — Work product reviews*
- ISO/IEC/IEEE 21839:2019 *Systems and software engineering — System of systems (SoS) considerations in life cycle stages of a system*

Please note that for the systems and software engineering of *product lines* and *product families*, additional standards apply.

[1] Please refer to the ISO Online Browsing Platform for more information on the various standards.
[2] Please note that standards flagged with FDIS, etc. are not yet published standards and as such only available to committee members.
[3] Please refer to the TU/e virtual library subscription on IEEE Xplore for any documents (also) published by IEEE.

Contents

Index

1. Terms with respect to *Trustworthiness in Artificial Intelligence* (AI)

Source: [4]

- *Artificial intelligence* is the *capability* of an engineered *system* to acquire, process and apply knowledge and skills.
- An *AI-based system* is a *system* including one or more components implementing AI.
- *Accountability* is the property that ensures that the actions of an *entity* may be traced uniquely to that *entity*.
- An *actor* is an *entity* that communicates and interacts.
- An *algorithm* is a set of rules for transforming the logical representation of *data*.
- An *asset* is anything that has *value* to a *stakeholder*.
- An *attribute* is a property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means.
- *Autonomy* is a characteristic of a *system* governed by its own rules as the result of self-learning. Such systems are not subject to *external control* or oversight.
- *Consistency* is the degree of *uniformity*, standardization and freedom from contradiction among the *documents* or parts of a *system* or component.
- *Control* is a purposeful action on or in a *process* to meet specified *objectives*.
- *Data* is re-interpretable representation of *information* in a formalized manner suitable for communication, interpretation or processing.
- The *data subject* is the individual about whom *personal data* are recorded.
- *Effectiveness* is the extent to which planned *activities* are realized and planned results achieved.
- *Efficiency* is the relationship between the results achieved and the resources used.
- An *entity* is any concrete or abstract thing of interest.
- *Harm* is an injury or damage to the health of people or damage to property or the environment.
- A *hazard* is a potential source of *harm*.
- *Information* is meaningful *data*.
- *Integrity* is the property of protecting the *accuracy* and completeness of *assets*.
- The *intended use* is the use in accordance with *information* provided with a *product* or *system* or, in the absence of such information, by generally understood *patterns* of usage.
- A *pattern* is a set of features and their relationships used to recognize an *entity* within a given context.
- *Personal data* is *data* relating to an identified or identifiable individual.
- *Privacy* is the freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of *data* about that individual.
- A *process* is a set of interrelated or interacting *activities* that use inputs to deliver an intended result.
- *Reliability* is a property of consistent intended behavior and results.
- A *risk* is an effect of *uncertainty* on *objectives*. 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*.
- A *robot* is a programmed actuated mechanism with a degree of *autonomy*, moving within its environment, to perform intended tasks. A robot includes the *control* system and interface of the *control system*.
- *Safety* is the freedom from *risk* which is not tolerable.
- *Security* is the degree to which a *product* or *system* protects *information* and *data* so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization.
- *Sensitive data* is *data* with potentially *harm*ful effects in the event of disclosure or misuse.
- A *stakeholder* is any individual, group or *organization* that can affect, be affected by or perceive itself to be affected by a decision or *activity*.
- A *system* is a combination of interacting elements organized to achieve one or more stated purposes.
- A *threat* is a potential cause of an unwanted incident, which may result in *harm* to *systems*, *organizations* or individuals.
- *Trust* is the degree to which a *user* or other *stakeholder* has confidence that a *product* or *system* will behave as intended.

[4] ISO/IEC TR 24028:2020 *Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence*

- *Trustworthiness* is the ability to meet *stakeholders*' expectations in a verifiable way. Depending on the context or sector and also on the specific *product* or service, *data* and technology used, different characteristics apply and need *verification* to ensure *stakeholders* expectations are met.
  Characteristics of *trustworthiness* include, for instance, *reliability*, *availability*, *resilience*, *security*, *privacy*, *safety*, *accountability*, *transparency*, *integrity*, *authenticity*, *quality*, *usability*.

- A *user* is an individual or group that interacts with a *system* or benefits from a system during its utilization.

- *Validation* is the confirmation, through the provision of *objective evidence*, that the *requirements* for a specific *intended use* or application have been fulfilled: the right *system* was built.

- *Value* <social> is belief(s) an *organization* adheres to and the standards that it seeks to observe.

- *Verification* is the confirmation, through the provision of *objective evidence*, that specified *requirements* have been fulfilled: the *system* was built right.

- A *vulnerability* is a weakness of an *asset* or *control* that can be exploited by one or more *threats*.

2. Terms with respect to *Testing AI-based systems*

Source: [5]

- *Adaptability* is the ability of a *system* to react to changes in its environment in order to continue meeting both functional and non-functional *requirements*.
- An AI-*based system* is a *system* including one or more components implementing AI.
- The AI *effect* is the situation when a previously labelled AI *system* is no longer considered to be AI as technology advances.
- *Artificial intelligence* (AI) is the *capability* of an engineered *system* to acquire, process and apply knowledge and skills.
- An *autonomous system* is a *system* capable of working without human intervention for sustained periods.
- *Autonomy* is the ability of a *system* to work for sustained periods without human intervention.
- A *deterministic system* is a *system* which, given a specific set of inputs and starting state, will always produce the same set of outputs and final state.
- *Explainability* <AI> is the level of understanding how the AI-*based system* came up with a given result
- *Flexibility* is the ability of a *system* to work in contexts outside its initial *specification* (i.e. change its behavior according to its actual situation to satisfy its *objectives*).
- *General* AI (*strong* AI) is AI that exhibits intelligent behavior comparable to a human across the full range of cognitive abilities.
- *Interpretability* <AI> is the level of understanding how the underlying (AI) technology works.
- *Machine learning* (ML) is a *process* using computational techniques to enable *systems* to learn from data or experience.
- *Narrow* AI (*weak* AI) is AI focused on a single well-defined *task* to address a specific problem.
- A *non-deterministic system* is a *system* which, given a specific set of inputs and starting state, will not always produce the same set of outputs and final state.
- A *probabilistic system* is a *system* whose behavior is described in terms of probabilities, such that its outputs cannot be perfectly predicted.
- A *regulatory standard* is a *standard* promulgated by a regulatory agency.
- A *robot* is a programmed actuated mechanism with a degree of *autonomy*, moving within its environment, to perform intended tasks.
  A robot includes the control system and interface of the control system.
- *Safety* is the expectation that a *system* does not, under defined *conditions*, lead to a state in which human life, health, property, or the environment is endangered.
- A *self-learning system* is an *adaptive system* that changes its behaviour based on learning from the practice of trial and error.
- A *simulator* <testing> is a device, computer program or *system* used during testing, which behaves or operates like a given *system* when provided with a set of controlled inputs.
- A *software agent* is a digital *entity* that perceives its environment and takes actions that maximize its chance of successfully achieving its goals.
- *Transparency* <AI> is the level of accessibility to the *algorithm* and *data* used by the AI-*based system*.

[5] ISO/IEC TR 29119-11:2020 *Software and systems engineering — Software testing — Part 11: Guidelines on the testing of AI-based systems*

3. Terms with respect to *Trustworthiness*

Source: [6]

- *Trustworthiness* is the ability to meet *stakeholders*' expectations in a *demonstrable*, *verifiable* and *measurable* way. Depending on the context or sector, and also on the specific *product* or *service*, data, and technology used, different characteristics apply and need *verification* to ensure *stakeholders*' expectations are met. *Characteristics* of *trustworthiness* include, for instance, *reliability*, *availability*, *resilience*, *security*, *privacy*, *safety*, *accountability*, *transparency*, *integrity*, *authenticity*, *quality*, *usability* and *accuracy*.

- *Accountability* <systems> is the property that ensures that actions of an *entity* can be traced uniquely to the entity.

- *Accountability* <governance> is the obligation of an individual or *organization* to account for its *activities*, for completion of a *deliverable* or *task*, accept the responsibility for those activities, deliverables or tasks, and to disclose the results in a transparent manner.

- *Accuracy* is a *measure* of closeness of results of observations, computations, or estimates to the true values or the values accepted as being true.

- *Authenticity* is the property that an *entity* is what it claims to be.

- *Availability* is the property of being accessible and usable upon demand by an authorized *entity*.

- *Integrity* <data> is [7] the property whereby *data* have not been altered in an unauthorized manner since they were created, transmitted or stored.

- *Integrity* <systems> is the property of accuracy and completeness.

- *Privacy* is the freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of *data* about that individual.

- *Quality* <data> is the degree to which the characteristics of *data* satisfy stated and implied needs when used under specified *conditions*.

- *Quality* <systems> is the degree to which all the properties and *characteristics* of a *product*, *process* or *service* satisfy the *requirements* which ensue from the purpose for which that product, process or service is to be used.

- *Reliability* is the ability of an item to perform as required, without *failure*, for a given time interval, under given *conditions*.

- *Resilience* is the *capability* of a *system* to maintain its functions and structure in the face of internal and external change, and to degrade gracefully when this is necessary.

- *Safety* is the expectation that a system does not, under defined *conditions*, lead to a state in which human life, health, property, or the environment is endangered.

- *Security* is the combination of *confidentiality*, *integrity* and *availability*.

- *Transparency* <information> is the open, comprehensive, accessible, clear and understandable presentation of *information*.

- *Transparency* <systems> is the property of a *system* or *process* to imply openness and *accountability*.

- *Usability* is the extent to which a *system*, *product* or *service* can be used by specified *users* to achieve specified *goals* with *effectiveness*, *efficiency* and satisfaction in a specified context of use.

- *Demonstrable* is the ability to communicate a characteristic of an *entity* in a convincing manner to an interested *stakeholder*.

- *Measurable* is the ability to assess an attribute of an *entity* against a *metric*.

- A *metric* is a defined measurement method and measurement scale.

- A *stakeholder* is any individual, group, or *organization* that can affect, be affected by, or perceive itself to be affected by a decision or *activity*.

- A *socio-technical system* is a *system* that includes a combination of technical and human or natural elements.

- A *system* is a combination of interacting elements organized to achieve one or more stated *purposes*.

- A *system-of-systems* is a set of *systems* and *system elements* that interact to provide a unique *capability* that none of the *constituent systems* can accomplish on its own. System elements can be necessary to facilitate interaction of the constituent systems in the system-of-systems.

[6] ISO/IEC NP TS 5723 *Systems Engineering – Trustworthiness Vocabulary*
[7] ISO/IEC 25012:2008 *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Data quality model*

4. Terms with respect to *Systems and Software Assurance*

Source: [8]

…

- *Assurance* is grounds for justified confidence that a *claim* has been or will be achieved.

- An *assurance case* is a reasoned, auditable *artefact* created that supports the contention that its top-level *claim* (or set of claims) is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claim(s).

  An *assurance case* contains the following and their relationships: one or more claims about properties, arguments that logically link the evidence and any assumptions to the claim(s), a body of evidence and possibly assumptions supporting these arguments for the *claim*(s), and justification of the choice of top-level claim and the method of reasoning.

- *Assurance information* is the *information* including a claim about a *system*, evidence supporting the *claim*, an argument showing how the evidence supports the achievement of the claim, and the context for these items.

- An *assurance objective* is a *purpose* of achievement of the assurance *claim*. Assurance objectives determine the required degree of *integrity level* and permissible uncertainty in the *assurance information*.

- The *integrity level* is the degree of confidence that the *system-of-interest* meets the associated *integrity level claim*. In this context, *integrity levels* are defined in terms of *risk* and hence cover *safety*, *security*, economic and any other dimension of *risk* that is relevant to the *system-of-interest*.

- The *integrity level requirements* is the set of *requirements* that, when met, will provide a level of confidence in the associated *integrity level claim* commensurate with the associated *integrity level*.

- An *integrity level claim* is a *proposition* representing a *requirement* on a *risk reduction measure* identified in the *risk treatment process* of the *system-of-interest*. In general, it is described in terms of *requirements* to avoid, *control* or *mitigate* the *consequences* of *dangerous conditions*, so as to provide a *tolerable risk* if it is met.

- A *risk reduction measure* is a *measure* to *reduce* or *mitigate risk*.

- A *desirable consequence* (*positive consequence*) is a *consequence* associated with a *benefit* or gain or avoiding an *adverse consequence*.

- An *error* is a discrepancy between a computed, observed or measured *value* or *condition*, and the true, specified or theoretically correct *value* or *condition*.

- A *fault* is a *defect* in a *system* or a representation of a *system* that if executed/activated can potentially result in an *error*. *Faults* can occur in *specifications* when they are not correct.

- An *attack* is a malicious *action* or *interaction* with the *system* or its *environment* that has the potential to result in a *fault* or an *error*, and thereby possibly in a *failure*, or an *adverse consequence*.

- A *violation* is a behaviour, act or *event* deviating from a *system*'s desired property or *claim* of interest.

- A *failure* is termination of the *ability* of a *system* to perform a required function or its inability to perform within previously specified limits; an externally visible deviation from the system's specification.

- A *systematic failure* is a *failure* related in a *deterministic* way to a certain cause that can only be eliminated by a modification of the design or of the manufacturing *process*, operational *procedures*, *documentation* or other relevant factors.

- The *approval authority* is the person (or persons) and/or *organization* (or *organizations*) responsible for approving activities, artefacts and other aspects of the *system* during its *life cycle*. It may include multiple *entities*, e.g., individuals or *organizations*. These can include different *entitles* with different levels of approval and/or different areas of interest.

- The *design authority* is the person or *organization* that is responsible for the *design* of the *product*.

- The *integrity assurance authority* is the independent person or *organization* responsible for *certifying compliance* with the *integrity level requirements*.

[8] ISO/IEC/IEEE 15026-1:2019 *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*

5. Terms with respect to *Systems and Software Engineering*

Source: [9]

- An *acquirer* is a *stakeholder* that acquires or procures a *product* or *service* from a supplier.
- *Acquisition* is a *process* of obtaining a *system*, *product* or *service*.
- An *activity* is a set of cohesive *tasks* of a *process*.
- An *agreement* is a mutual acknowledgement of terms and conditions under which a working relationship is conducted.
- An *audit* is an independent examination of a *work product* or set of *work products* to *assess compliance* with *specifications*, *standards*, contractual *agreements*, or other criteria.
- A *baseline* is a formally approved version of a *configuration item*, regardless of media, formally designated and fixed at a specific time during the *configuration item*'s *life cycle*.
- A *business process* is partially ordered set of enterprise *activities* that can be executed to achieve some desired end-result in pursuit of a given *objective* of an *organization*.
- A *configuration item* is an *item* or aggregation of hardware, software, or both, that is designated for *configuration management* and treated as a single *entity* in the *configuration management* process.
- A *customer* is an *organization* or person that receives a *product* or *service*.
- To *design* <process> is to define the *architecture*, *system elements*, interfaces, and other *characteristics* of a *system* or *system element*.
- A *design* is the result of the design *process*. *Information*, including *specification* of *system elements* and their relationships, that is sufficiently complete to support a *compliant* implementation of the *architecture*. *Design* provides the detailed implementation-level physical structure, behaviour, temporal relationships, and other *attributes* of *system elements*.
- A *design characteristic* is one of the *design attributes* or distinguishing *features* that pertain to a *measurable* description of a *product* or *service*.
- An *enabling system* is a *system* that supports a *system-of-interest* during its *life cycle stages* but does not necessarily contribute directly to its function during operation. Each *enabling system* has a *life cycle* of its own.
- An *environment* <system> is the context determining the setting and circumstances of all influences upon a *system*.
- A *facility* is physical means or equipment for facilitating the performance of an action, e.g., buildings, instruments, tools.
- An *incident* is an anomalous or unexpected *event*, set of *events*, *condition*, or situation at any time during the *life cycle* of a *project*, *product*, *service*, or *system*.
- An *information item* is a separately identifiable body of information that is produced, stored, and delivered for human use.
- An *infrastructure* is a hardware and software environment to support computer system and software design, development, and modification.
- A *life cycle* is the evolution of a *system*, *product*, *service*, *project* or other human-made *entity* from conception through *retirement*.
- A *life cycle model* is a *framework* of *processes* and *activities* concerned with the *life cycle*, which can be organized into *stages*, acting as a common reference for communication and understanding.
- An *organization* is a group of people and *facilities* with an arrangement of *responsibilities*, *authorities* and relationships.
- A *party* is an *organization* entering into an *agreement*.
- A *problem* is a difficulty, *uncertainty*, or otherwise realized and undesirable *event*, set of *events*, *condition*, or situation that requires investigation and *corrective action*.
- A *process* is a set of interrelated or interacting *activities* that transforms *inputs* into *outputs*.
- A *process outcome* is an observable result of the *successful* achievement of the *process purpose*.
- The *process purpose* is a high-level *objective* of performing the *process* and the likely *outcomes* of *effective* implementation of the *process*. The *purpose* of

[9] ISO/IEC/IEEE 12207:2017 *Systems and software engineering — Software life cycle processes*

implementing the *process* is to provide *benefits* to the *stakeholders*.

- A *product* is the result of a *process*.
- A *project* is an endeavour with defined start and finish *criteria* undertaken to create a *product* or *service* in accordance with specified resources and requirements. A project is sometimes viewed as a unique process comprising coordinated and controlled *activities* and composed of *activities* from the Technical Management *processes* and Technical *processes* defined in this document.
- *Portfolio* <project> is a collection of *projects* that addresses the *strategic objectives* of the *organization*.
- *Qualification* is the *process* of demonstrating whether an *entity* is *capable* of fulfilling specified *requirements*.
- *Quality assurance* is part of *quality management* focused on providing confidence that *quality requirements* will be fulfilled.
- A *quality characteristic* is an inherent *characteristic* of a *product*, *process* or *system* related to a *requirement*. Critical quality characteristics commonly include those related to health, safety, security assurance, reliability, availability and supportability.
- *Quality management* is the coordinated activities to direct and control an *organization* with regard to *quality*.
- A *release* is a particular version of a *configuration item* that is made available for a specific *purpose*.
- A *requirement* is a statement that translates or expresses a *need* and its associated *constraints* and *conditions*.
- A *resource* is an *asset* that is utilized or consumed during the execution of a *process*. Resources include those that are reusable, renewable or consumable.
- *Retirement* is the withdrawal of active support by the operation and maintenance *organization*, partial or total replacement by a new *system*, or installation of an upgraded system.
- *Safety* is the expectation that a *system* does not, under defined *conditions*, lead to a *state* in which human life, health, property, or the environment is endangered.
- *Security* is the protection against intentional subversion or forced *failure*; a composite of four *attributes*: *confidentiality*, *integrity*, *availability*, and *accountability* plus aspects of a fifth, *usability*, all of which have the related issue of their *assurance*.
- A *service* is a performance of *activities*, *work*, or duties. It is self-contained, coherent, discrete, and can be composed of other services. It is generally an intangible product.
- A *software element* is a *system element* that is *software*.
- *Software engineering* [10]is the application of a systematic, disciplined, quantifiable approach to the development, operation, and maintenance of software; that is, the application of engineering to software.
- A *software item* is source code, object code, control code, control data, or a collection of these items.
- A *software product* is a set of computer programs, procedures, and possibly associated documentation and data. A *software product* is a *software system* viewed as the *output* (*product*) resulting from a *process*.
- A *software system* is a *system* for which software is of primary importance to the *stakeholders*. In the most general case, a *software system* is comprised of hardware, software, people, and manual procedures. In a *software system*, software is the leading driver in meeting *system requirements*.
- A *software system element* is a member of a set of elements that constitute a *software system*. It can include one or more *software units*, *software elements*, hardware units, hardware elements, *services*, and other *system elements* and *systems*. It can be viewed as a *system element*.
- A *software unit* is an atomic-level software component of the software *architecture* that can be subjected to standalone testing.
- A *stage* is a period within the *life cycle* of an *entity* that relates to the *state* of its description or realization. As used in this *document*, *stages* relate to major *progress* and achievement *milestones* of the *entity* through its *life cycle*. *Stages* often overlap.
- A *stakeholder* is an individual or *organization* having a right, share, claim, or interest in a *system* or in its possession of *characteristics* that meet their needs and expectations. Some stakeholders can have interests that oppose each other or oppose the system.

[10] ISO/IEC TR 19759:2015 *Software Engineering — Guide to the software engineering body of knowledge*

- A *supplier* is an *organization* or an individual that enters into an agreement with the *acquirer* for the supply of a *product* or *service*.

- A *system* is a combination of interacting *elements* organized to achieve one or more stated *purposes*. A *system* is sometimes considered as a *product* or as the *services* it provides. In practice, the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g., aircraft system or database management system. Alternatively, the word "system" is substituted simply by a context-dependent synonym, e.g., aircraft or database, though this potentially obscures a system principles perspective. A *system* can include the associated equipment, facilities, material, software, firmware, technical documentation, services and personnel required for operations and support to the degree necessary for use in its intended environment.

- A *system element* is a member of a set of elements that constitute a *system*. It is a discrete part of a *system* that can be implemented to fulfil specified *requirements*.

- A *system-of-interest* is a *system* whose *life cycle* is under consideration.

- A *system-of-systems* (SoS) is a set of *systems* that integrate or interoperate to provide a unique *capability* that none of the *constituent systems* can accomplish on its own. Each *constituent system* is a useful *system* by itself, having its own management, goals, and resources, but coordinates within the SoS to provide the unique capability of the SoS.

- *Systems engineering* is the interdisciplinary approach governing the total technical and managerial effort required to transform a set of *stakeholder needs*, expectations, and *constraints* into a solution and to support that solution throughout its life.

- A *task* is a required, recommended, or permissible action, intended to contribute to the achievement of one or more *outcomes* of a *process*.

- *Technical management* is the application of technical and administrative resources to plan, organize and control engineering functions.

- A *trade-off* is decision-making actions that select from various *requirements* and alternative solutions on the basis of net *benefit* to the *stakeholders*.

- *Traceability* is the degree to which a relationship can be established among two or more logical entities, especially entities having a predecessor-successor or master-subordinate relationship to one another, such as requirements, system elements, verifications, or tasks.

- A *user* is an individual or group that interacts with a *system* or *benefits* from a *system* during its utilization.

- *Validation* is confirmation, through the provision of *objective evidence*, that the *requirements* for a specific *intended use* or *application* have been fulfilled.

- *Verification* is confirmation, through the provision of *objective evidence*, that specified *requirements* have been fulfilled.

Source: [11]

...

- An *architecture* is a fundamental *organization* of a *system* embodied in its components, their relationships to each other, and to the environment, and the principles guiding its *design* and *evolution*.

- A *baseline* is a *specification* or *work product* that has been *formally reviewed* and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal *change control* procedures.

- An *operator* is an *entity* that performs the *operations* of a *system*. The role of operator and the role of user may be vested, simultaneously or sequentially, in the same individual or organization.

- An *organization* is a person or a group of people and *facilities* with an arrangement of responsibilities, authorities and relationships.

- A *request for tender* is a *document* used by the *acquirer* as the means to announce its intention to potential bidders to *acquire* a specified *system product* or *service*.

- *Security* is all aspects related to defining, achieving, and maintaining confidentiality, *integrity*, availability, non-repudiation, accountability, authenticity, and *reliability* of a *system*.

[11] ISO/IEC/IEEE 15288:2015 *Systems and software engineering — System life cycle processes*

Source: [12]

…

- *Ad-hoc reviewing* is an unstructured independent *review* technique.
- An *author check* is an *informal review* performed by the *author* of the *work product*.
- *Checklist-based reviewing* is a *review* technique guided by a list of questions or required *attributes*.
- A *formal review* is a form of *review* that follows a defined *process* with formal documented *output*.
- An *informal review* is a form of *review* that does not follow a defined *process* and has no formal documented *output*.
- An *inspection* is a *formal review* of a *work product* to identify *issues*, which uses defined team roles and *measurement* to *improve* the *review process*.
- An *issue* is an observation that deviates from expectations.
- A *milestone review* is a *formal review* of a *work product* and supporting evidence used to determine its acceptability for use in the next stage of development or for delivery. The *requirement* for this form of *review* is normally specified in the *project plan*.
- *Page-by-page reviewing* is a technique where reviewers *review* a *work product* in a sequential order.
- A *peer review* is a review of *work products* performed by others qualified to do the same work.
- *Perspective-based reading* is form of *role-based reviewing* that uses checklists and involves the creation of prototype *deliverables* to check the completeness and other *quality characteristics* of the *work product*.
- *Role-based reviewing* is a technique where reviewers *review* a *work product* from the perspective of different stakeholder roles.
- *Scenario-based reviewing* is a technique where the *review* is guided by determining the *ability* of the *work product* to address specific *scenarios*.
- A *technical review* is a *formal peer review* of a *work product* by a team of technically qualified *personnel* that examines the suitability of the *work product* for its *intended use* and identifies discrepancies from *specifications* and *standards*. A technical review may also provide recommendations of alternatives and examination of various alternatives.
- A *walkthrough* is a *formal review* in which an *author* leads members of the *review* through a *work product*, and the participants ask questions and make comments about possible *issues*.
- A *work product* is an *artefact* produced by a *process*.

[12] ISO/IEC 20246:2017 *Software and systems engineering — Work product reviews*

6. Terms with respect to *Systems-of-Systems*

Source: [13]

…

- A *constituent system* is an independent system that forms part of a *system-of-systems*. A *constituent system* can be part of one or more *systems-of-systems*. Each *constituent system* is a useful system by itself, having its own development, management, utilization, goals, and resources, but interacts within the *system-of-systems* to provide the unique *capability* of the *system-of-systems*.
- A *system* is a combination of interacting elements organized to achieve one or more stated *purposes*.
- A *system element* is member of a set of elements that constitutes a *system*. A *system element* is a discrete part of a *system* that can be implemented to fulfil specified *requirements*.
- A *system-of-interest* is a *system* whose *life cycle* is under consideration in a specific context.
- A *system-of-systems* is a set of *systems* and *system elements* that interact to provide a unique *capability* that none of the *constituent systems* can accomplish on its own.

[13] ISO/IEC/IEEE 21839:2019 *Systems and software engineering — System of systems (SoS) considerations in life cycle stages of a system*

7. Terms with respect to *Systems Integrity*

Source: [14]

...

- An *adverse consequence* is a *consequence* that results in a specified level of loss. It results from the *system-of-interest* being in a *dangerous condition* combined with the environment of the *system* being in its worst-case state.

- A *claim* is a true-false statement about the limitations on the values of an unambiguously defined property — called the claim's property — and limitations on the uncertainty of the property's values falling within these limitations during the claim's duration of applicability under stated *conditions*.

  A claim potentially contains the following: property of the system-of-interest, limitations on the value of the property associated with the claim (e.g., on its range), limitations on the uncertainty of the property value meeting its limitations, limitations on duration of claim's applicability, duration-related uncertainty, limitations on conditions associated with the claim, and condition-related uncertainty.

- A *consequence* is an *outcome* of an *event* affecting *objectives*.

- A *dangerous condition* is a state of a *system* that, in combination with some states of the environment, will result in an *adverse consequence*.

  The concept of *dangerous conditions* is introduced in order to cover not only hazardous situations in the safety context but also *errors* in the *reliability*, *integrity*, *confidentiality* or *dependability* contexts and other states of a system which can lead to adverse consequences. A *dangerous condition* therefore has at least the following *attributes*: the associated adverse consequences, the trigger events that lead to the dangerous condition, and the trigger events that lead to the adverse consequences from the dangerous condition.

- An *integrity level* is the required degree of confidence that the *system-of-interest* meets the associated *integrity level claim*.

- An *integrity level claim* is a *claim* representing a *requirement* for a *risk reduction measure* identified in the *risk treatment* process of the *system-of-interest*.
  In general, it is described in terms of *requirements* that, when met, would avoid, *control* or *mitigate* the *consequences* of *dangerous conditions* and provide *tolerable risk*.

- An *integrity level requirement* is a set of *requirements* that, when met, will provide a level of confidence in the associated *integrity level claim* commensurate with the associated *integrity level*.

- The *initial risk* is the *estimated risk* before applying *risk reduction measures*.

- The *level of risk* is the *magnitude of a risk* or combination of risks, expressed in terms of the combination of *consequences* and their *likelihood*.

- The *likelihood* is the probability of something happening.

- A *property-of-interest* is any property that, if lost, is considered a negative effect.
  The concept of property-of-interest is introduced in order to characterize negative effects of *consequences*.

- The *residual risk* is the risk remaining after *risk treatment*.

- A *risk* is an effect of uncertainty on objectives. An effect is a deviation from the expected: positive and/or negative. Typically, the focus is on negative deviations leading to *adverse consequences*.

- *Uncertainty* is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

- *Risk criteria* are the terms of reference against which the *significance of a risk* is evaluated.

- A *risk reduction measure* is a *measure* taken to reduce or mitigate risk.

- A *risk source* is an element that, alone or in combination, has the intrinsic potential to give rise to *risk*.

- *Risk treatment* is the *process* to eliminate *risk* or reduce it to a *tolerable level*.

- The *target risk* is the *risk* that is intended to be reached.

- A *threat agent* is an *entity* that can adversely act on *property-of-interest*.

[14] ISO/IEC 15026-3:2015 *Systems and software engineering — Systems and software assurance — Part 3: System integrity levels*

- *Tolerable risk* is the *level of risk* that is accepted in a given context based on the current values of society. A tolerable risk is sometimes called acceptable risk.

- A *condition* is *measurable* qualitative or quantitative *attribute* that is stipulated for a *requirement* and that indicates a circumstance or event under which a *requirement* applies

- A *constraint* is an externally imposed limitation on the *system*, its *design*, or *implementation* or on the *process* used to develop or modify a system. A constraint is a factor that is imposed on the solution by force or compulsion and may limit or modify the design.

- The *dependability* <of an item> is the ability to perform as and when required.
  Dependability includes *availability*, *reliability*, *recoverability*, *maintainability*, and maintenance support performance, and, in some cases, other characteristics such as durability, safety and security.

- A *process* is a set of interrelated or interacting *activities* that transforms inputs into outputs.

- A *process view* is a description of how a specified *purpose* and set of *outcomes* may be achieved by employing the *activities* and *tasks* of existing *processes*.

- A *product* is a result of a *process*.

- A *requirement* is a statement which translates or expresses a *need* and its associated *constraints* and *conditions*. A *requirement* is an expression of one or more particular *needs* in a very specific, precise and unambiguous manner.

8. Terms with respect to *Big Data*

Source: [15]

- A *benefit* is an advantage to the organization of the actionable knowledge derived from an analytic system. It is often ascribed to big data due to the understanding that data has potential value that was typically not considered previously.
- *Big data* is *extensive datasets* — primarily in the *data* characteristics of *volume*, *variety*, *velocity*, and/or *variability* — that require a scalable technology for efficient storage, manipulation, management, and analysis.
- *Data analytics* is a composite concept consisting of data acquisition, data collection, data validation, *data processing*, including data quantification, data visualization, and data interpretation. It is used to understand objects represented by *data*, to make predictions for a given situation, and to recommend on steps to achieve objectives.
- A *database* is a collection of *data* organized according to a conceptual structure describing the characteristics of these data and the relationships among their corresponding entities, supporting one or more application areas.
- A *data model* is a pattern of structuring *data* in a *database* according to the formal descriptions in its *information system* and according to the requirements of the database management system to be applied.
- *Data processing* is the systematic performance of operations upon *data*. Examples are arithmetic or logic operations upon data, merging or sorting of data, or operations on text, such as editing, sorting, merging, storing, retrieving, displaying, or printing.
- *Data science* is the extraction of actionable knowledge from *data* through a process of discovery, or hypothesis and hypothesis testing.
- A *data set* (*dataset*) is an identifiable collection of *data* available for access or download in one or more formats.
- A *data type* (*datatype*) is a defined set of *data* objects of a specified data structure and a set of permissible operations, such that these data objects act as operands in the execution of any one of these operations.
- *Data variability* is changes in transmission rate, format or structure, semantics, or quality of *datasets*.
- *Data variety* is the range of formats, logical models, timescales, and semantics of a *dataset*. It refers to irregular or heterogeneous data structures, their navigation, query, and data typing.
- *Data velocity* is the rate of flow at which *data* is created, transmitted, stored, analysed or visualised.
- *Data veracity* is the completeness and/or accuracy of data. It refers to descriptive data and self-inquiry about objects to support real-time decision-making.
- *Data volatility* is the characteristic of *data* pertaining to the rate of change of these data over time.
- *Data volume* is the extent of the amount of *data* relevant to impacting computation and storage resources and their management during *data processing*. It becomes important in dealing with large *datasets*.
- *Distributed data processing* is *data processing* in which the performance of operations is dispersed among the nodes in a computer network.
- Metadata is data about data or data elements, possibly including their data descriptions, and data about data ownership, access paths, access rights and data volatility.
- *Non-relational database* is a *database* that does not follow a *relational model*.
- *Non-relational model* is a *logical datamodel* that does not follow a *relational model* for the storage and manipulation of *data*.
- A *relational database* is a *database* in which the *data* are organized according to a *relational model*.
- A *relational model* is a *data model* whose structure is based on a set of relations.
- *Streaming data* is *data* passing across an interface from a source that is operating continuously.
- *Structured data* is *data* which are organized based on a pre-defined (applicable) set of rules.
- *Unstructured data* is *data* which are characterized by not having any structure apart from that record or file level.

[15] ISO/IEC 20546:2019 *Information technology — Big data — Overview and vocabulary*

9. Terms with respect to *Cloud*

Source: [16]

...

- A *party* is a natural person or legal person, whether or not incorporated, or a group of either.
- A *service level agreement* (SLA) is a documented *agreement* between the *service provider* and *customer* that identifies *services* and *service targets*. A service level agreement can be included in a *contract* or another type of documented *agreement*.
- An *application capabilities type* is a *cloud capabilities type* in which the *cloud service customer* can use the *cloud service provider*'s *applications*.
- *Cloud application portability* is the *ability* to *migrate* an *application* from one *cloud service* to another *cloud service*.
- A *cloud auditor* is a *cloud service partner* with the responsibility to conduct an *audit* of the provision and use of *cloud services*.
- A *cloud capabilities type* is a classification of the functionality provided by a *cloud service* to the *cloud service customer*, based on resources used. The *cloud capabilities types* are *application capabilities type*, *infrastructure capabilities type* and *platform capabilities type*.
- *Cloud computing* is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.
- *Cloud data portability* is *data portability* from one *cloud service* to another *cloud service*.
- A *cloud deployment model* is a way in which *cloud computing* can be organized based on the control and sharing of physical or virtual resources. The *cloud deployment models* include *community cloud*, *hybrid cloud*, *private cloud* and *public cloud*.
- A *cloud service* is one or more capabilities offered via *cloud computing* invoked using a defined interface.
- A *cloud service broker* is a *cloud service partner* that negotiates relationships between *cloud service customers* and *cloud service providers*.
- A *cloud service category* is a group of *cloud services* that possess some common set of *qualities*. It can include capabilities from one or more *cloud capabilities types*.
- A *cloud service customer* is a *party* which is in a business relationship for the purpose of using *cloud services*.
- *Cloud service customer data* is a class of data objects under the control, by legal or other reasons, of the *cloud service customer* that were input to the *cloud service*, or resulted from exercising the capabilities of the *cloud service* by or on behalf of the *cloud service customer* via the published interface of the *cloud service*. Please note that an example of legal controls is copyright. It may be that the *cloud service* contains or operates on data that is not cloud service customer data; this might be data made available by the *cloud service providers*, or obtained from another source, or it might be publicly available data. However, any output data produced by the actions of the *cloud service customer* using the capabilities of the *cloud service* on this data is likely to be *cloud service customer data*, following the general principles of copyright, unless there are specific provisions in the *cloud service* agreement to the contrary.
- *Cloud service derived data* is a class of data objects under *control* of the *cloud service provider* that are derived as a result of interaction with the *cloud service* by the *cloud service customer*. It includes log data containing records of who used the service, at what times, which functions, types of *data* involved and so on. It can also include *information* about the numbers of authorized users and their *identities*. It can also include any configuration or customization data, where the *cloud service* has such configuration and customization capabilities.
- A *cloud service partner* is a *party* which is engaged in support of, or auxiliary to, activities of either the *cloud service provider* or the *cloud service customer*, or both.
- A *cloud service provider* is a *party* which makes *cloud services* available.
- *Cloud service provider data* is a class of data objects, specific to the operation of the *cloud service*, under the *control* of the *cloud service provider*. It includes but is not limited to resource configuration and utilization information, *cloud service* specific virtual machine, storage and network resource allocations, overall data centre configuration and utilization, physical and virtual resource failure rates, operational costs and so on.
- A *cloud service user* is a natural person, or entity acting on their behalf, associated with a *cloud service customer* that uses *cloud services*. Examples of such *entities* include *devices* and *applications*.

[16] ISO/IEC 17788:2014 *Information technology — Cloud computing — Overview and vocabulary*

- *Communications as a Service* (CaaS) is a *cloud service category* in which the *capability* provided to the *cloud service customer* is real time interaction and collaboration. It can provide both *application capabilities type* and *platform capabilities type*.

- A *community cloud* is a *cloud deployment model* where *cloud services* exclusively support and are shared by a specific collection of *cloud service customers* who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection.

- *Compute as a Service* (CompaaS) is a *cloud service category* in which the capabilities provided to the *cloud service customer* are the provision and use of processing resources needed to deploy and run software. To run some software, capabilities other than processing resources may be needed.

- *Data portability* is the *ability* to easily transfer data from one *system* to another without being required to re-enter data. It is the ease of moving the data that is the essence here. This might be achieved by the source system supplying the data in exactly the format that is accepted by the target system. But even if the formats do not match, the transformation between them may be simple and straightforward to achieve with commonly available tools. On the other hand, a process of printing out the data and rekeying it for the target system could not be described as "easy".

- *Data Storage as a Service* (DSaaS) is a *cloud service category* in which the *capability* provided to the *cloud service customer* is the provision and use of data storage and related capabilities. DSaaS can provide any of the three *cloud capabilities types*.

- A *hybrid cloud* is a *cloud deployment model* using at least two different *cloud deployment models*.

- *Infrastructure as a Service* (IaaS) is a *cloud service category* in which the *cloud capabilities type* provided to the *cloud service customer* is an *infrastructure capabilities type*. The *cloud service customer* does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The *cloud service customer* may also have limited ability to control certain networking components (e.g., host firewalls).

- An *infrastructure capabilities type* is a *cloud capabilities type* in which the *cloud service customer* can provision and use processing, storage or networking resources.

- A *measured service* is a *metered delivery* of *cloud services* such that usage can be monitored, controlled, reported and billed.

- *Multi-tenancy* is the allocation of physical or virtual resources such that multiple *tenants* and their computations and data are isolated from and inaccessible to one another.

- *Network as a Service* (NaaS) is a *cloud service category* in which the *capability* provided to the *cloud service customer* is transport connectivity and related network capabilities. NaaS can provide any of the three *cloud capabilities types*.

- *On-demand self-service* is a feature where a *cloud service customer* can provision computing capabilities, as needed, automatically or with minimal interaction with the *cloud service provider*.

- *Platform as a Service* (PaaS) is a *cloud service category* in which the *cloud capabilities type* provided to the *cloud service customer* is a *platform capabilities type*.

- A *platform capabilities type* is a *cloud capabilities type* in which the *cloud service customer* can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the *cloud service provider*.

- A *private cloud* is a *cloud deployment model* where *cloud services* are used exclusively by a single *cloud service customer* and resources are controlled by that *cloud service customer*.

- A *public cloud* is a *cloud deployment model* where *cloud services* are potentially available to any *cloud service customer* and resources are controlled by the *cloud service provider*.

- *Resource pooling* is the aggregation of a *cloud service provider*'s physical or virtual resources to serve one or more *cloud service customers*.

- *Reversibility* is the process for *cloud service customers* to retrieve their *cloud service customer data* and *application* artefacts and for the *cloud service provider* to delete all *cloud service customer data* as well as contractually specified *cloud service derived data* after an agreed period.

- *Software as a Service* (SaaS) is a *cloud service category* in which the *cloud capabilities type* provided to the *cloud service customer* is an *application capabilities type*.

- A *tenant* is one or more *cloud service users* sharing access to a set of physical and virtual resources.

10. Terms with respect to *Requirements*

Source: [17]

...

- An *acquirer* is a *stakeholder* that acquires or procures a *product* or *service* from a *supplier*.
- An *attribute* is an inherent property or *characteristic* of an *entity* that can be distinguished quantitatively or qualitatively by human or automated means.
- A *baseline* is a formally approved version of a *configuration item*, regardless of media, formally designated and fixed at a specific time during the *configuration item*'s *life cycle*.
- A *business requirements specification* is structured collection of the *requirements* (business or mission problem or opportunity definition, concepts, and required conditions of solutions) of the business or mission and its relation to the *external environment*.
- A *concept of operations* is a verbal and graphic statement, in broad outline, of an *organization*'s assumptions or intent in regard to an operation or series of operations. It frequently is embodied in long-range strategic plans and annual operational plans. In the latter case, the concept of operations in the plan covers a series of connected operations to be carried out simultaneously or in succession. The concept is designed to give an overall picture of the organization operations.
- A *condition* is a *measurable* qualitative or quantitative *attribute* that is stipulated for a *requirement* and that indicates a circumstance or event under which a *requirement* applies.
- A *constraint* is an externally imposed limitation on the *system*, its design, or implementation or on the *process* used to *develop* or modify a *system*. A constraint is a factor that is imposed on the solution by force or compulsion and may limit or modify the design.
- A *context of use* is the users, tasks, equipment (hardware, software and materials), and the physical and social environments in which a *product* is used.
- A *customer* is a person or *organization* that could or does receive a *product* or a *service* that is intended for or required by this person or *organization*. Customers are a subset of stakeholders. A customer can be internal or external to the organization.
- A *derived requirement* is a *requirement* deduced or inferred from the collection and organization of requirements into a particular system configuration and solution. A *derived requirement* is typically identified during the *elicitation* of stakeholder requirements, requirements analysis, trade studies or validation.
- A *developer* is an individual or *organization* that performs development *activities* (including requirements analysis, design, testing through acceptance) during the *system* or *software life-cycle process*.
- A *document* is a uniquely identified unit of *information* for human use. A *document* can be a single *information item*, or part of a larger *information item*.
- *Human systems integration* is the interdisciplinary technical and management *processes* for integrating human considerations within and across all *system elements*.
- An *information item* [18] is a separately identifiable body of *information* that is produced, stored, and delivered for human use.
- A *level of abstraction* is a view at a specific level of detail in a description of a *system*.
- An *operational concept* is a verbal and graphic statement of an *organization*'s assumptions or intent in regard to an operation or series of operations of a specific system or a related set of specific new, existing or modified systems. The operational concept is designed to give an overall picture of the operations using one or more specific systems, or set of related systems, in the organization's operational environment from the *users*' and *operators*' perspective. It is what the enterprise or *organization* intends to achieve.
- An *operational scenario* is a description of an imagined sequence of *events* or *activities* that includes the interaction of the *product* or *service* with its *environment* and *users*, as well as interaction among its *product* or *service* components when there is end-use significance. Such *operational scenarios* are used to evaluate the *requirements* and design of the system and to verify and validate the system.
- An *operator* is an individual or organization that performs the operations of a system. The role of operator and the role of user can be vested, simultaneously or sequentially, in the same individual or organization. An individual operator combined with knowledge, skills

[17] ISO/IEC/IEEE 29148:2018 *Systems and software engineering — Life cycle processes — Requirements engineering*
[18] ISO/IEC/IEEE 15289:2019 *Systems and software engineering — Content of life-cycle information items* (documentation)

and procedures can be considered as an element of the system. An operator may perform operations on a system that is operated, or of a system that is operated, depending on whether or not operating instructions are placed within the system boundary.

- A *requirement* is a statement which translates or expresses a need and its associated *constraints* and *conditions*. Requirements exist at different levels in the system structure. A *requirement* is an expression of one or more particular needs in a very specific, precise and unambiguous manner.

- *Requirements elicitation* is the use of systematic techniques, such as prototyping and structured surveys, to proactively identify and document *customer* and end *user* needs.

- *Requirements engineering* is the interdisciplinary function that mediates between the domains of the *acquirer* and *supplier* to establish and maintain the *requirements* to be met by the *system*, *software* or *service* of interest. It is concerned with discovering, eliciting, developing, analysing, verifying, validating, communicating, documenting and managing *requirements*.

- *Requirements management* is the *activities* that identify, document, maintain, communicate, trace and track *requirements* throughout the *life cycle* of a *system*, *product* or *service*.

- *Requirements traceability* is the identification and documentation of the derivation path (upward) and allocation/flow-down path (downward) of *requirements* in the requirements set.

- The *requirements traceability matrix* is the structured *information artefact* that links *requirements* to their higher level requirements or needs or to lower level implementation.

- *Requirements validation* is the *confirmation* that requirements (individually and as a set) define the right system as intended by the *stakeholders*.

- *Requirements verification* is the *confirmation* by examination that *requirements* (individually and as a set) are well-formed. This means that a *requirement* or a set of requirements has been *reviewed* to help ensure the *characteristics* of good *requirements* are achieved and the requirements set is well organized.

- A *software requirements specification* is a structured collection of the essential *requirements* [functions, performance, design constraints and *attributes*] of the software and its external interfaces.

- A *stakeholder* is an individual or *organization* having a right, share, claim or interest in a *system* or in its possession of *characteristics* that meet their needs and expectations.

- A *stakeholder requirements specification* is a structured collection of the *requirements* [*characteristics*, *context*, *concepts*, *constraints* and priorities] of the *stakeholder* and the relationship to the external *environment*.

- A *state* is a *condition* that characterizes the behaviour of a function, subfunction or element at a point in time.

- A *supplier* is an *organization* or individual that enters into an *agreement* with the *acquirer* for the supply of a product or service.

- A *system-of-interest* is a *system* whose *life cycle* is under consideration in the context of this *document*.

- A *system requirements specification* is a structured collection of the *requirements* [functions, performance, design *constraints*, and other *attributes*] for the *system* and its *operational environments* and external interfaces

- A *trade-off* is decision-making actions that select from various *requirements* and alternative solutions on the basis of net *benefit* to the *stakeholders*.

- A *user* is an individual or group that interacts with a system or *benefits* from a *system* during its utilization.

- *Validation* is the *confirmation*, through the provision of *objective evidence*, that the *requirements* for a specific intended use or application have been fulfilled. *Validation* in a *system life cycle* context is a set of *activities* ensuring and gaining confidence that a system is able to accomplish its intended use, goals and objectives. The right *system* has been built.

- *Verification* is the *confirmation*, through the provision of *objective evidence*, that *specified requirements* have been fulfilled. *Verification* in a *system life cycle* context is a set of *activities* that compares a *product* of the *system life cycle* against the required *characteristics* for that *product*. This may include, but is not limited to, specified *requirements*, design description and the *system* itself. The *system* has been built right.

11. Terms with respect to *Architecture Description* (AD)

Source: [19]

…

- *Architecting* is the *process* of conceiving, defining, expressing, documenting, communicating, certifying proper implementation of, maintaining and improving an *architecture* throughout a *system*'s *life cycle*.

  Architecting takes place in the context of an organization ("person or a group of people and facilities with an arrangement of responsibilities, authorities and relationships") and/or a project ("endeavour with defined start and finish criteria undertaken to create a product or service in accordance with specified resources and requirements").

- An *architecture* is the fundamental concepts or properties of a *system* in its *environment* embodied in its elements, relationships, and in the principles of its design and evolution.

- An *architecture description* (AD) is a *work product* used to express an *architecture*.

- An *architecture framework* is the conventions, principles and practices for the description of *architectures* established within a specific domain of application and/or community of *stakeholders*.

- An *architecture view* is a *work product* expressing the *architecture* of a *system* from the perspective of specific system *concerns*.

- An *architecture viewpoint* is a *work product* establishing the conventions for the construction, interpretation and use of *architecture views* to frame specific system *concerns*.

- A *concern* is an interest in a system relevant to one or more of its *stakeholders*. A concern pertains to any influence on a system in its environment, including developmental, technological, business, operational, organizational, political, economic, legal, regulatory, ecological and social influences.

- The *environment* is the *context* determining the setting and circumstances of all influences upon a system. The environment of a system includes developmental, technological, business, operational, organizational, political, economic, legal, regulatory, ecological and social influences.

- A *model kind* is the conventions for a type of modelling.

- A *stakeholder* is an individual, team, organization, or classes thereof, having an interest in a system.

[19] ISO/IEC/IEEE 42010:2011 *Systems and software engineering — Architecture description*

12. Terms with respect to *Architecture*

Source: [20]

- *Architecting* is the conceiving, defining, expressing, documenting, communicating, certifying proper implementation of, maintaining and improving an *architecture* (3.2) throughout the life cycle of an *entity-of-interest*.

- An *architecture* is the fundamental concepts or properties related to an *entity* in its *environment* and governing principles for the realization and evolution of this *entity* and its related *life cycle processes*.

- An *architecture aspect* is a unit of modularization of concerns within an *architecture description*, capturing *characteristics* or features of the *entity-of-interest*. Aspects enable the architect to analyse, address and structure *architecture concerns*. In general, there is a many-to-many relation between *aspects* and *concerns*. An aspect can pertain either to an entity of interest, to an architecture, or to an environment (such as to a situation or action).

- An *architecture description* (AD) is a *work product* used to express an *architecture*. It is a tangible representation of information provided to the stakeholders. In other words, it can also be considered as an *information item*.

- An *architecture description element* is a part of an *architecture description* that expresses the architecture. Elements include *stakeholders*, *concerns*, *perspectives*, and *aspects* identified in an AD, and *views*, *view components*, *viewpoints*, and *model kinds* included in an AD.

- An *architecture description framework* (ADF) is the conventions, principles and practices for the description of *architectures* established within a specific domain of application or *community* of *stakeholders*.

- An *architecture description language* (ADL) is a means of expression, with syntax and semantics, consisting of a set of representations, conventions, and associated rules intended to be used to describe an *architecture*.

- An *architecture view* is an *information item*, governed by an *architecture viewpoint*, comprising part of an *architecture description*. A *viewpoint* is a frame of reference for the *concerns* determined by the architect as relevant to the purpose of the *architecture description*.

- An *architecture viewpoint* is the conventions for the creation, interpretation and use of an *architecture view* to frame one or more *concerns*.

- A *concern* is a matter of relevance or importance to a *stakeholder* regarding an *entity-of-interest*. Stated concerns are useful when relevant to the purpose of the architecting effort and refer to specific rather than categorical *difficulties*, *problems*, or *requirements*.

- A *correspondence* is an expression of a relationship among *architecture description elements* or *among architecture descriptions*. Correspondences are used to express a wide range of relationships, such as equivalence, composition, refinement, consistency, traceability, dependency, constraint, satisfaction, and obligation.

- An *entity-of-interest* is a subject of an *architecture description*.

- The *environment* is the aggregate of surrounding *things*, *conditions*, contexts of, or influences upon an *entity-of-interest*. It includes external entities that can have various influences upon the entity of interest, such as developmental, technological, business, operational, organizational, political, economic, legal, regulatory, ecological and social influences as well as external physical effects such as electromagnetic radiation, charged particles, gravitational effects, and electric and magnetic fields. A label attached as a qualifier to the word environment identifies a particular context within that environment, such as development environment, test environment, and operational environment. It would be more correct to refer to these as development context, test context, operational context, etc. A context can be to help understand an entity or its architecture, including the derivation of an architecture.

- To *frame* is to formulate or construct in a particular style or language.

- An *information item* is a separately identifiable body of information that is produced, stored, and delivered for human and machine use.

- A *model kind* is a category of *model* distinguished by its key characteristics and modelling conventions.

- A *specification* is an *information item* that identifies, in a complete, precise and verifiable manner, the *requirements*, *design*, behaviour, or other expected *characteristics* of a *system*, *service*, or *process*.

[20] ISO/IEC/IEEE DIS 42010 *Software, systems and enterprise — Architecture description*

- A *stakeholder* is a role, position, individual, organization or classes thereof, having an interest, right, share, or claim, in an *entity* or its *architecture*.

- A *stakeholder perspective* is a way of thinking about an *entity*, especially as it relates to *concerns*. The way one thinks about an entity can be influenced by one's beliefs, training, experience, knowledge, personality, character traits, culture, peer pressure, role or stance etc.

- A *view component* (*architecture view component*) is a separable portion of one or more *architecture views* that is governed by the applicable *model kind* or legend.

Source: [21]

- *Architecting* is the conceiving, defining, expressing, documenting, communicating, certifying proper implementation of, maintaining and improving an *architecture* throughout the *life cycle* for an *architecture entity*.

- An *architecture* is the fundamental concepts or properties of an *entity* in its *environment* and governing principles for the realization and evolution of this *entity* and its related *life cycle processes*. The fundamental concepts or properties of the *architecture entity* are usually intended to be embodied in the *entity*'s components, the relationships between components, and the relationships between the *entity* and its *environment*. Representation of the concepts or properties of an entity and governing principles is captured in *architecture models*.

- An *architecture collection* is a group of *architectures* held by an *organization* that is subject to *governance* and *management* by the *organization* as a whole.

- An *architecture entity* is a *thing* being considered, described, discussed, studied or otherwise addressed during the *architecting* effort. The following are kinds of *architecture entities* that can be dealt with by the *architecture processes*: *enterprise*, *organization*, solution, *system* (including *software systems*), subsystem, business, data (as a data element or data structure), *application*, information technology (as a collection), mission, *product*, *service*, software item, hardware item, *product line*, family of systems, *system-of-systems*, collection of systems, collection of applications, etc.

- An *architecture framework* is the conventions, principles and practices for use by *architecture*-related *activities* that have been established within a specific domain of *application* or *community* of *stakeholders*.

- A *concern* is a matter of interest or importance to a *stakeholder*. Examples are affordability, agility, availability, dependability, flexibility, maintainability, reliability, resilience and viability are examples of concerns.

- An *enterprise* is a bold or complex endeavour. One or more *organizations* can participate in an enterprise. In case of multi-organization enterprises, each of the organizations brings various resources forward for use in the enterprise and they participate to the extent that they benefit from their involvement. The purpose of the enterprise is to address some challenges that these participating organizations cannot readily address on their own. Within a single organization, an enterprise may refer to a subset of the organization which is typically addressing particularly challenging or complex issues, often over a defined duration, and may undertake this with certain relaxations, tightening or otherwise authorized modifications of standard corporate *processes* and practices.

- A *library* is a place containing collections of *work products* and useful *information items* for people to read, borrow or refer to, and for machines to access and retrieve data from. In a *repository*, *work products* and other items are preserved for future retrieval when needed, whereas in a library, working data is temporarily stored and retrieved as necessary.

- A *life cycle* <entity> is a set of distinguishable *phases* or *stages* that an *entity* goes through from its conceptualization until it ceases to exist.

- A *life cycle* <architecture> is a set of distinguishable *phases* or *stages* that an *architecture* goes through. The architecture life cycle starts with the identification of a need for the architecture and ends when it is no longer needed.

- A *model* is an abstract representation of an *entity* or collection of *entities* that provides the *ability* to portray, understand or predict the properties or *characteristics* of the *entity* or collection under *conditions* or situations of interest. A model can use a formalism that could be based on mathematical or scientific principles and concepts. A model can be generated using an established metamodel. Metamodels are often used to facilitate development of accurate, complete, consistent and understandable models. A *model* can be used to construct or express *architecture views* of the *entity*. Descriptive models and analytic models are two kinds of models. A model should be governed by a *model kind*.

[21] ISO/IEC/IEEE 42020:2019 *Software, systems and enterprise — Architecture processes*

- A *phase* is a period of time in the *life cycle* during which *activities* are performed that enable achievement of *objectives* for that *phase*.

- A *registry* is a book or *system* for keeping an official list or *record* of *work products* and the associated *information items*. *Repository* and *library* items should be recorded in *registries* to enable better *management* and *governance* of these *items*.

- A *repository* is a place where *work products* and the associated *information items* are or can be stored for preservation and retrieval. *Repository items* should be under *configuration control*.

- A *stakeholder* is a role, position, individual or *organization* having a right, share, claim or other interest in an *architecture entity* or its *architecture* that reflects their needs and expectations.

- A *system* is a combination of interacting elements organized to achieve one or more stated *purposes*. A system is sometimes considered as a product or as a set of services. A *system element* is a discrete part of a *system* that can be implemented to fulfil specified *requirements*. A system element can be hardware, software, data, humans, processes (e.g., processes for providing service to users), procedures (e.g., operator instructions), facilities, materials, and naturally occurring entities (e.g., water, organisms, minerals), or any combination. A *system* can be comprised of multiple subsystems. For example, an aircraft system can include an avionics subsystem and a radar subsystem. The distinction between a system and a subsystem is a matter of perspective, and as such the radar subsystem can be referred to as a radar system in some contexts.

- A *task* is a recommended action intended to contribute to the achievement of one or more *outcomes* of an *architecture process*.

- A *view* <architecture> is an *information item* expressing the *architecture* from the perspective of specific *stakeholders* regarding specific *aspects* of the *architecture entity* and its *environment*.

- A *viewpoint* <architecture> is the conventions for the construction, interpretation and use of *architecture views* to address specific *concerns* about the *architecture entity*.

- A *work product* is artefact associated with the execution of a *process*.

Source: [22]

- An *architecture evaluation* (AE) is a judgment about one or more *architectures* with respect to the specified evaluation *objectives*. Various kinds of judgments could be made during an *architecture evaluation*, such as validating that architectures address the *concerns* of *stakeholders*, assessing the *quality* of *architectures* with respect to their *intended purpose*, assessing the *value* of *architectures* or *architecture entities* to their *stakeholders*, determining whether *architecture entities* address their *intended purpose*, providing knowledge and information about *architecture entities* and identifying *risks* and *opportunities* associated with *architectures*.

- An *architecture evaluation framework* is the conventions, principles and practices for *evaluating architectures* in a consistent and repeatable manner.

- A *factor* is a circumstance, fact or influence that contributes to a *result* or *outcome*. It is something that contributes causally to a result. Factors identification can sometimes be driven by knowledge of desired effects.

- A *value* is a regard that something is held to deserve; the importance, worth, or usefulness of something to somebody. *Architecture evaluation* is focused primarily on the *value* of an *architecture* with respect to *stakeholder concerns* or *architecture objectives* for that *thing*. However, sometimes the purpose of the evaluation effort is, by inference, to determine the *impact* of the *architecture* on the *value* of the *architecture entity* when the *entity* is developed or evolved to align with the *architecture* concepts and properties. The determination of architecture value can take various aspects into account, such as worth, significance, importance, usefulness, benefit, and quality. Even though a new architecture could be found to be of greater value with respect to the current situation, this needs to be balanced against the costs and risks of adopting the new architecture. So, it is not necessarily the case that when examining architecture alternatives, the one with the maximum value is proposed as the preferred choice since the extra cost or risk of this architecture might not be worth the extra burden. This is sometimes referred to as the benefit-cost ratio or some other term with similar meaning.

[22] ISO/IEC/IEEE 42030:2019 *Software, systems and enterprise — Architecture evaluation framework*

13. Terms with respect to *Agile*

Source: [23]

Also see: [24], [25]

...

- *Agile development* is a development approach based on *iterative development*, frequent *inspection* and adaptation, and incremental deliveries in which *requirements* and solutions evolve through collaboration in cross-functional teams and through continuous *stakeholder* feedback.
- An *agile environment* is an organizational culture, *infrastructure*, and methodologies that support *agile development*.
- An *agile team* is an *organization* or team using *agile development* methods and approaches.
- A *backlog* is a collection of agile *features* or stories of both functional and non-functional *requirements* that are typically sorted in an order based on value priority.
- '*Done*' is regarded by the *agile team* as complete and ready to use.
- An *epic* is a major collection of related *feature* sets broken down into individual *features* or *user stories* and implemented in parts over a longer period of time.
- A *feature* is a functional or non-functional distinguishing *characteristic* of a *system*.
- An *information developer* is a person who prepares content for *information* for users.
- An *information development lead* is a person who leads the activities of preparing information for users.
- An *iteration* is a short time frame in which a set of software *features* is developed, leading to a working product that can be demonstrated to *stakeholders*.
- An *iterative development* is a repeated use of concurrent planning, developing, and testing activities.
- A *persona* is a model of a user with defined characteristics, based on research.
- A *stand-up meeting* is a brief daily project status or planning meeting used in *agile development* methodologies.
- A *use case* is a description of behavioural *requirements* of a *system* and its interaction with a user. A *use case* describes the users' goal and the requirements including the sequence of interactions between users and the system.
- A *user story* is a simple narrative illustrating a user requirement from the perspective of a *persona*.

[23] ISO/IEC/IEEE 26515:2018 *Systems and software engineering — Developing information for users in an agile environment*
[24] ISO/IEC CD TR 29110-5-4 *Systems and software engineering — Lifecycle profiles for Very Small Entities (VSEs) — Part 5-4: Agile software development guidelines*
[25] ISO/IEC CD TR 29119-6 *Software and systems engineering — Software testing — Part 6: Guidelines for the use of ISO/IEC/IEEE 29119 in Agile projects*

14. Terms with respect to *Maintenance*

Source: [26]

…

- *Adaptive maintenance* is a modification of a software product, performed after delivery, to keep a software product usable in a changed or changing environment. It provides enhancements necessary to accommodate changes in the *environment* in which a software product must operate. These changes are those that must be made to keep pace with the changing environment.

- *Additive maintenance* is a modification of a software product performed after delivery to add additional functionality or features to enhance the usage of the product.

- *Corrective maintenance* is a reactive modification of a software product performed after delivery to correct discovered problems. It repairs the software product to satisfy requirements.

- *Emergency maintenance* is an unscheduled fix performed to temporarily keep a system operational pending corrective maintenance.

- *Maintainability* is the degree of *effectiveness* and *efficiency* with which a product or system can be modified by the intended maintainers. *Modifications* can include corrections, improvements or adaptation of the software to changes in *environment*, and in *requirements* and functional *specifications*. Modifications include those carried out by specialized support staff, and those carried out by business or operational staff, or end users. It includes installation of updates and upgrades. It Maintainability can be interpreted as either an inherent capability of the product or system to facilitate maintenance activities, or the quality in use experienced by the maintainers for the goal of maintaining the product or system.

- An *enhancement* is software change that is a new requirement. There are two types of software enhancements, *adaptive* and *perfective*.

- A *Modification Request* (MR) is a generic term used to identify proposed changes to a software product that is being maintained. It may later be classified as a correction or enhancement and identified as corrective, preventive, adaptive, or perfective maintenance. MRs are also referred to as change requests.

- *Perfective maintenance* is a modification of a software product after delivery to detect and correct latent faults in the software product before they are manifested as *failures*. It provides enhancements for users, improvement of program documentation, and recoding to improve software performance, maintainability, or other software attributes.

- *Preventive maintenance* is a modification of a software product after delivery to detect and correct latent *faults* in the software product before they occur in the live system.

- A *Problem Report* (PR) is a term used to identify and describe problems detected in a software product. PRs are either submitted directly to denote faults, or they are established after impact analysis is performed on Modification Reports and faults are found.

- *Software maintenance* is the totality of activities required to provide support to a *software system*. Activities are performed during the pre-delivery stage as well as the post-delivery stage.

- *Software sustainment* is the comprehensive requirements to support, maintain and operate the software *capabilities* of a *system*. It includes *processes*, *procedures*, people, material and *information* required to support, maintain and operate the *software aspects* of a *system*.

- *Software transition* is a controlled and coordinated sequence of actions wherein *software development* passes from the *organization* performing *software development* to the *organization* performing *software maintenance*.

[26] ISO/IEC/IEEE CD2 14764 (Ed3) *Software Engineering — Software Life Cycle Processes — Maintenance*

15. Terms with respect to *Risk Management*

Source: [27]

...

- A *risk management process* is a systematic application of management *policies*, *procedures* and practices to the *activities* of communicating, consulting, establishing the context, and identifying, analysing, evaluating, *treating*, *monitoring* and *reviewing risk*.

- *Communication* and *consultation* are continual and iterative processes that an *organization* conducts to provide, share or obtain *information*, and to *engage* in dialogue with *stakeholders* regarding the management of *risk*. The *information* can relate to the existence, nature, form, *likelihood*, significance, evaluation, acceptability and *treatment* of the management of risk.

- *Consultation* is a two-way process of informed communication between an *organization* and its *stakeholders* 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.

- A *stakeholder* is a person or *organization* that can affect, be affected by, or perceive themselves to be affected by a decision or *activity*.

- The *risk perception* is a *stakeholder*'s view on a *risk*. It reflects the *stakeholder*'s *needs*, issues, knowledge, *belief* and *values*.

- *Establishing the context* is defining the external and internal parameters to be considered when managing *risk*, setting the *risk scope* and *risk criteria* for the risk management *policy*.

- The *external context* is the external environment in which the *organization* seeks to achieve its *objectives*. It can include: the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; key drivers and trends having *impact* on the *objectives* of the *organization*; and relationships with, and perceptions and values of external *stakeholders*.

- The *internal context* is the internal environment in which the *organization* seeks to achieve its *objectives*. It can include: *governance*, organizational structure, roles and *accountabilities*; *policies*, *objectives*, and the *strategies* that are in place to achieve them; the *capabilities*, understood in terms of resources and knowledge (e.g. capital, time, people, *processes*, *systems* and technologies); information systems, information flows and decision-making processes (both formal and informal); relationships with, and perceptions and values of internal *stakeholders*; the organization's culture; standards, guidelines and models adopted by the organization; and form and extent of contractual relationships.

- *Risk criteria* are terms of reference against which the significance of a *risk* is evaluated. These are based on organizational *objectives*, and *external* and *internal context*. These can be derived from standards, laws, *policies* and other *requirements*.

- A *risk assessment* is an overall *process* of *risk identification*, *risk analysis* and *risk evaluation*. It is the process of finding, recognizing and describing *risks*. It involves the identification of *risk sources*, *events*, their causes and their potential *consequences*. It can involve historical data, theoretical analysis, informed and expert opinions, and *stakeholder*'s needs.

- A *risk description* is a structured statement of *risk* usually containing four elements: *sources*, *events*, *causes* and *consequences*.

- A *risk source* is an element which alone or in combination has the intrinsic potential to give rise to *risk*. It can be tangible or intangible.

- An *event* is an occurrence or change of a particular set of circumstances. It can be one or more occurrences and can have several causes. It can consist of something not happening. It can sometimes be referred to as an "incident" or "accident". An event without *consequences* can also be referred to as a "near miss", "incident", "near hit" or "close call".

- A *hazard* is a *source* of potential *harm*. A hazard can be a *risk source*.

- The *risk owner* is the person or *entity* with the *accountability* and *authority* to manage a *risk*.

- *Risk analysis* is a process to comprehend the nature of *risk* and to determine the *level of risk*. It provides the basis for *risk evaluation* and decisions about *risk treatment*. It includes risk estimation.

- *likelihood* is a chance of something happening. In risk management terminology, the word "likelihood" is used to refer to the chance of something happening

[27] ISO Guide 73:2009

whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically [such as a *probability* or a *frequency* over a given time period].

- *Exposure* is the extent to which an *organization* and/or *stakeholder* is subject to an *event*.

- A *consequence* is an *outcome* of an *event* affecting *objectives*. An *event* can lead to a range of *consequences*. A *consequence* can be certain or uncertain and can have positive or negative effects on *objectives*. *Consequences* can be expressed qualitatively or quantitatively. Initial *consequences* can escalate through knock-on effects.

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

- The *frequency* is the number of *events* or outcomes per defined unit of time. It can be applied to past *events* or to potential future *events*, where it can be used as a *measure* of *likelihood*/*probability*.

- A *vulnerability* is set of intrinsic properties of something resulting in susceptibility to a *risk source* that can lead to an *event* with a *consequence*.

- A *risk matrix* is a tool for ranking and displaying *risks* by defining ranges for *consequence* and *likelihood*.

- A *level of risk* is the magnitude of a *risk* or combination of risks, expressed in terms of the combination of *consequences* and their *likelihood*.

- A *risk evaluation* is a *process* of comparing the results of *risk analysis* with *risk criteria* to determine whether the *risk* and/or its magnitude is acceptable or *tolerable*. It assists in the decision about *risk treatment*.

- The *risk attitude* is the *organization*'s approach to assess and eventually pursue, retain, take or turn away from *risk*. It is the amount and type of *risk* that an *organization* is willing to pursue or retain.

- The *risk tolerance* is an *organization*'s or *stakeholder*'s readiness to bear the *risk* after *risk treatment* in order to achieve its *objectives*. It can be influenced by legal or regulatory *requirements*.

- *Risk aversion* is an *attitude* to turn away from *risk*.

- *Risk aggregation* is the combination of a number of risks into one *risk* to develop a more complete understanding of the overall risk.

- *Risk acceptance* is an informed decision to take a particular *risk*. It can occur without *risk treatment* or during the process of *risk treatment*. Accepted risks are subject to *monitoring* and *review*.

- *Risk treatment* is a *process* to modify *risk*. It can involve: avoiding the *risk* by deciding not to start or continue with the *activity* that gives rise to the *risk*; taking or increasing *risk* in order to pursue an opportunity; removing the *risk source*; changing the *likelihood*; changing the *consequences*; sharing the *risk* with another party or parties [including contracts and *risk financing*]; and retaining the *risk* by informed decision. Risk treatments that deal with negative consequences are sometimes referred to as "*risk mitigation*", "risk elimination", "risk prevention" and "risk reduction". Risk treatment can create new risks or modify existing risks.

- *Control* is a *measure* that is modifying *risk*. Controls include any *process*, *policy*, device, practice, or other *actions* which modify *risk*. Controls may not always exert the intended or assumed modifying effect.

- *Risk avoidance* is an informed decision not to be involved in, or to withdraw from, an *activity* in order not to be exposed to a particular *risk*. It can be based on the result of *risk evaluation* and/or legal and regulatory obligations.

- *Risk sharing* is a form of *risk treatment* involving the agreed distribution of *risk* with other parties. Legal or regulatory requirements can limit, prohibit or mandate *risk sharing*. It can be carried out through insurance or other forms of contract. The extent to which *risk* is distributed can depend on the *reliability* and clarity of the sharing arrangements.

- *Risk transfer* is a form of *risk sharing*.

- *Risk financing* is a form of *risk treatment* involving contingent arrangements for the provision of funds to meet or modify the financial *consequences* should they occur.

- *Risk retention* is the acceptance of the potential *benefit* of gain, or burden of loss, from a particular *risk*. It includes the acceptance of *residual risks*. The *level of risk* retained can depend on *risk criteria*.

- *Residual risk* is *risk* remaining after *risk treatment*. It can contain unidentified risk. It can also be known as "retained risk".

- *Resilience* is an *adaptive* capacity of an *organization* in a complex and changing environment.

- *Monitoring* is continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected. It can be applied to a *risk management framework*, *risk management process*, *risk* or *control*.

- A *review* is an *activity* undertaken to determine the suitability, adequacy and *effectiveness* of the subject matter to achieve established objectives. It can be applied to a *risk management framework*, *risk management process*, *risk* or *control*.
- *Risk reporting* is a form of *communication* intended to inform particular internal or external *stakeholders* by providing *information* regarding the current state of *risk* and its *management*.
- A *risk register* is a *record* of *information* about identified *risks*. The term "risk log" is sometimes used instead of "risk register".

Source: [28]

- The *risk exposure* is the potential loss presented to an individual, *project*, or *organization* by a *risk*. Risk exposure is commonly defined as the product of a *probability* and the magnitude of a *consequence*, that is, an expected value or expected exposure.
- The *risk threshold* is the *measure* of the level of *uncertainty* or the level of *impact* at which a *stakeholder* may have a specific interest. Below that *risk threshold*, the *organization* will accept the *risk*. Above that *risk threshold*, the *organization* will not tolerate the *risk*. It also is the *condition* that triggers some *stakeholder* action. Different risk thresholds can be defined for each *risk*, *risk category* or combination of *risks*, based on differing *risk criteria*.
- The *risk tolerance* is the degree, amount, or volume of *risk* that an *organization* or individual will withstand.

Source: [29]

- The *probability* [30] is the extent to which an *event* is likely to occur. *Frequency* rather than *probability* may be used in describing *risk*. Degrees of *belief* about *probability* can be chosen as classes or ranks.
- The *project risk profile* is a *project*'s current and historical risk-related information; a compendium or aggregate of all of the individual *risk profiles* in a *project*. It includes the *risk management context*, along with the chronological *record* of *risks* and their individual *risk profiles*, priority ordering, risk-related measures, treatment status, contingency plans, and *risk action requests*. A *project risk profile* consists of a collection of the risk profiles of all the individual risks, which in turn includes the current and historical *risk states*.
- A *risk* is the combination of the *probability* of an *event* and its *consequence*. The term "risk" is generally used only when there is at least the possibility of negative consequences.
- A *risk profile* is a description of any set of *risks*. Such a set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.
- A *risk management audit* is a systematic, independent and documented *process* for obtaining evidence and evaluating it objectively in order to determine the extent to which the *risk management framework*, or any selected part of it, is adequate and effective.
- A *risk action request* is the recommended *treatment* alternatives and supporting *information* for one or more *risks* determined to be above a *risk threshold*.
- A *risk category* is a class or type of risk (e.g., technical, legal, organizational, safety, economic, engineering, cost, schedule).
- A *risk management plan* is a description of how the elements and resources of the *risk management process* will be implemented within an *organization* or *project*.
- A *risk management process* is a continuous *process* for systematically identifying, analysing, *treating*, and *monitoring risk* throughout the *life cycle* of a *product* or *service*.
- A *risk management system* is set of elements of an *organization*'s *management system* concerned with managing *risk*. Management system elements can include strategic planning, decision making, and other processes for dealing with risk.

[28] ISO 31000:2018 *Risk management — Guidelines*
[29] ISO/IEC/IEEE 16085 *Systems and software engineering — Life cycle processes — Risk management*
[30] ISO 3534-1:2006 *Statistics — Vocabulary and symbols — Part 1: General statistical terms and terms used in probability*

- A *risk profile* is a chronological record of a *risk*'s current and historical *risk state* information.
- The *risk state* is the current *project* risk information relating to an individual *risk*. Such information concerning an individual risk may include the current description, *causes*, *probability*, *consequences*, estimation scales, confidence of the estimates, *treatment*, *threshold*, and an estimate of when the risk will reach its *threshold*.
- A *risk threshold* is a *condition* that triggers some *stakeholder* action. Different risk thresholds may be defined for each *risk*, *risk category* or combination of risks based upon differing *risk criteria*.
- A *risk treatment* is the *process* of selection and implementation of *measures* to modify *risk*. The term "risk treatment" is sometimes used for the measures themselves. Risk treatment measures can include *avoiding*, *optimizing*, *transferring* or *retaining* risk.
- A *source* is an *item* or *activity* having a potential for a *consequence*. In the context of *safety*, *source* is a *hazard*.
- A *stakeholder* is any individual, group or *organization* that can affect, be affected by, or perceive itself to be affected by, a risk.

16. Terms with respect to organizations

Source: various

- An *organization* is a group of people and facilities with an arrangement of *responsibilities*, *authorities* and relationships.
- An *organization* is a person or group of people that has its own functions with *responsibilities*, *authorities*, and relationships to achieve its *objectives*.
- A *stakeholder* is an individual or *organization* having a right, share, claim, or interest in a *system* or in its possession of *characteristics* that meet their *needs* and expectations.
- A *consequence* is the *outcome* of an *event* affecting one or more *stakeholders*. An *event* can lead to a range of *consequences*. A *consequence* can be certain or uncertain and can have positive or negative effects on *objectives*. Consequences can be expressed qualitatively or quantitatively. Initial *consequences* can escalate through follow-on effects.

17. Terms with respect to project management

Source: [31]

- A *risk*
- .

[31] ISO/…

18. Terms with respect to *Internet-of-Things*

Source: [32]

...

- An *application* is software designed to fulfil a particular *purpose*.
- *Availability* is the property of being *accessible* and *usable* upon demand by an authorized *entity*.
- A *characteristic* is an abstraction of a property of an *entity* or of a set of entities.
- *Cloud computing* is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.
- A *cloud service* is one or more *capabilities* offered via *cloud computing* invoked using a defined interface.
- *Compliance* is the *characteristic* of *conformance* to rules, such as those defined by a law, a regulation, a standard, or a *policy*.
- A *component* is a modular, deployable, and replaceable part of a *system* that encapsulates implementation and exposes a set of interfaces.
- *Confidentiality* is the property that *information* is not made available or disclosed to unauthorized individuals, *entities*, or *processes*.
- A *data store* is a persistent repository for digital *information*. A data store can be accessed by a single *entity* or shared by multiple entities via a network or other connection.
- A *digital entity* is a computational and/or data element. It can exist as a *cloud service* or as a *service* in a data center, or as a network element or as an IoT *gateway*.
- A *digital user* is a *digital entity* that uses an IoT *system*. It includes automation *services* that act on behalf of *human users*.
- A *discovery service* is a *service* to find unknown resources, *entities* or *services* based on a *specification* of the desired target.
- An *endpoint* is a *component* that exposes or uses one or more network interfaces.
- An *entity* is a thing (physical or non-physical) having a distinct existence.
- A *functional component* is a functional building block needed to engage in an *activity*, backed by an implementation. See also "*component*", which is a superset containing all functional components and other types of component that are deployable.
- A *human user* is a natural person who uses a *system*.
- An *identifier* is *information* that unambiguously distinguishes one entity from other entities in a given *identity context*.
- An *identity context* is an environment where an *entity* can use a set of attributes for identification.
- An *interface* is a shared boundary between two *functional components*, defined by various *characteristics* pertaining to the functions, physical interconnections, signal exchanges, and other *characteristics*, as appropriate.
- *Interoperability* is the ability of two or more systems or applications to exchange information and to mutually use the *information* that has been exchanged.
- A *network* is an *infrastructure* that connects a set of *endpoints*, enabling communication of *data* between the *digital entities* reachable through them.
- A *physical entity* is an *entity* that has material existence in the physical world. In the Internet of Things *reference architecture*, the *physical entity* is the thing to be sensed and/or actuated by IoT *devices* or IoT *systems*.
- A *reference architecture* is an *architecture description* that provides a proven template solution when developing or validating an architecture for a particular solution.
- A *service* is a distinct part of the functionality that is provided by an *entity* through *interfaces*.
- A *service provider* is an *organization* or part of an *organization* that manages and delivers a *service* or services to the *customer*.
- A *stakeholder* is an individual, team, *organization*, or classes thereof, having an interest in a *system*.
- *Trustworthiness* is the property of deserving trust or confidence.
- A *virtual entity* is a *digital entity* that represents a *physical entity*.
- *Internet of Things* (IoT) is the *infrastructure* of interconnected *entities*, people, *systems* and *information* resources together with *services* which processes and

[32] ISO/IEC 20924:2018 *Information technology — Internet of Things (IoT) — Vocabulary*

reacts to *information* from the physical world and virtual world.

- An *actuator* is an IoT *device* that changes one or more properties of a *physical entity* in response to a valid input.
- An IoT *conceptual model* is a common structure and definitions for describing the concepts, relationships, and behavior within an IoT *system*.
- An IoT *device* is an *entity* of an IoT *system* that interacts and communicates with the physical world through sensing or actuating.
- An IoT *device* can be a *sensor* or an *actuator*.
- An IoT *domain* is a major *functional group* of an IoT *system*. Every *entity* in an IoT *system* participates in one or more IoT *domains* and is said to be included or contained by that *domain*. The IoT *domain* consists of six *domains*: user domain, operation & management domain, application & service domain, resource access & interchange domain, sensing & controlling domain, physical entity domain.
- An IoT *gateway* is an *entity* of an IoT *system* that connects one or more proximity networks and the IoT *devices* on those networks to each other and to one or more access networks.
- An IoT *system* is a *system* providing functionalities of Internet of Things. An IoT *system* is inclusive of IoT *devices*, IoT *gateways*, *sensors*, and *actuators*.
- An IoT *user* is a *user* of an IoT *system*. An IoT *user* can be a *human user* or a *digital user*.
- A *sensor* is an IoT *device* that measures one or more properties of one or more physical entities and *outputs* digital data that can be transmitted over a network.
- IoT *trustworthiness* is the property of deserving *trust* or confidence within the entire *lifecycle* of an Internet of Things implementation to ensure *security*, *privacy*, *safety*, *reliability* and *resiliency*.

19. Terms with respect to Internet-of-Things

Source: [33]

…

- This is text of the first column. This is text of the first column. This is text of the first column. This is text of the first column. This is text of the first column. This is text of the first column. This is text of the first column. This is text of the first column. This is text of the first column. This is text of the first column. This is text of the first column. This is text of the first column. This is text of the first column. This is text of the first column. This

[33] ISO/IEC 20924:2018 *Information technology — Internet of Things (IoT) — Vocabulary*

20. Terms with respect to *Quality Management Systems*

Source: [34]

...

- An *activity* <project management> is the smallest identified *object* of *work* in a *project*.
- An *association* is an *organization* consisting of member *organizations* or persons.
- The *context of the organization* is the combination of internal and external issues that can influence an organization's approach to developing and achieving its *objectives*. The organization's *objectives* can be related to its *products* and *services*, investments and behavior towards its *interested parties*. In English, this concept is often referred to by other terms such as "business environment", "organizational environment" or "ecosystem of an organization". Understanding the *infrastructure* can help to define the *context of the organization*.
- *Continual improvement* is a recurring *activity* to enhance *performance*.
  The *process* of establishing *objectives* and finding opportunities for *improvement* is a *continual process* using *audit findings* and *audit conclusions*, analysis of *data*, *management reviews* or other means and generally leads to *corrective action* or *preventive action*.
- A *customer* is a person or *organization* that could or does receive a *product* or a *service* that is intended for or required by this person or *organization*.
- *Engagement* is *involvement* in, and contribution to, activities to achieve shared *objectives*.
- *Involvement* is taking part in an *activity*, event or situation.
- A *management system* is a set of interrelated or interacting elements of an *organization* to establish *policies* and *objectives*, and *processes* to achieve those *objectives*. The *management system* elements establish the organization's structure, roles and responsibilities, planning, operation, policies, practices, rules, beliefs, objectives and processes to achieve those *objectives*.
- An *organization* is a person or group of people that has its own functions with *responsibilities*, *authorities* and relationships to achieve its *objectives*.
- An *interested party* (*stakeholder*) is a person or *organization* that can affect, be affected by, or perceive itself to be affected by a decision or *activity*.
- A *provider* (*supplier*) is an *organization* that provides a *product* or *a service*.
- An *external provider* (*external supplier*) is a *provider* that is not part of the *organization*.
- *Improvement* is an *activity* to enhance *performance*.
- *Management* is the set of coordinated *activities* to *direct* and *control* an *organization*.
  Management can include establishing *policies* and *objectives*, and *processes* to achieve these *objectives*.
- A *metrological function* is a functional unit with administrative and technical responsibility for defining and implementing the measurement *management system*.
- *Quality assurance* is part of *quality management* focused on providing confidence that *quality requirements* will be fulfilled.
- *Quality control* is part of *quality management* focused on fulfilling *quality requirements*.
- *Quality management* is the *management* regarding *quality*.
  It can include establishing *quality policies* and *quality objectives*, and *processes* to achieve these *quality objectives* through *quality planning*, *quality assurance*, *quality control*, and *quality improvement*.
- *Quality improvement* is part of *quality management* focused on increasing the ability to fulfil *quality requirements*. These *quality requirements* can be related to any aspect such as *effectiveness*, *efficiency*, or *traceability*.
- The *quality management system* is part of a *management system* with regard to *quality*.
- *Quality management system realization* is the *process* of establishing, documenting, implementing, maintaining and continually improving a *quality management system*.
- *Quality planning* is part of *quality management* focused on setting *quality objectives* and specifying necessary operational processes, and related resources to achieve the *quality objectives*. Establishing *quality plans* can be part of *quality planning*.
- *Configuration management* is the set of coordinated *activities* to direct and control *configuration*.
  It generally concentrates on technical and organizational activities that establish and maintain control of a *product* or *service* and its *product configuration information* throughout the *life cycle* of the *product*.

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

- *Change control* <configuration management> is the set of activities for *control* of the *output* after formal approval of its product configuration information.

- *Project management* is *planning*, *organizing*, *monitoring*, *controlling* and *reporting* of all aspects of a *project*, and the motivation of all those involved in it to achieve the project *objectives*.

- A *configuration object* is an *object* within a *configuration* that satisfies an end-use function.

- A *process* is a set of interrelated or interacting *activities* that use *inputs* to deliver an *intended result*.
  Processes in an *organization* are generally planned and carried out under controlled *conditions* to add value.
  A *process* where the *conformity* of the resulting output cannot be readily or economically validated is frequently referred to as a "special process".

- A *project* is a unique *process*, consisting of a set of coordinated and controlled *activities* with start and finish dates, undertaken to achieve an *objective* conforming to specific *requirements*, including the *constraints* of time, cost and resources. An individual *project* can form part of a larger project structure and generally has a defined start and finish date. In some *projects* the *objectives* and *scope* are updated, and the *product* or *service characteristics* defined progressively as the project proceeds.

- The *top management* is the person or group of people who *directs* and *controls* an *organization* at the highest level. Top management has the power to delegate *authority* and provide resources within the organization. If the scope of the *management system* covers only part of an *organization*, then *top management* refers to those who direct and control that part of the organization.

- *Competence acquisition* is the *process* of attaining *competence*.

- A *procedure* is a specified way to carry out an *activity* or a *process*.

- To *outsource* is to make an arrangement where an external *organization* performs part of an organization's function or *process*.

- A *contract* is a binding agreement

- *design and development* is the set of *processes* that transform *requirements* for an *object* into more detailed requirements for that *object*. The *requirements* forming input to *design and development* are often the result of research and can be expressed in a broader, more general sense than the *requirements* forming the *output* of *design and development*. The *requirements* are generally defined in terms of *characteristics*. In a *project* there can be several *design and development stages*.

- A *system* is a set of interrelated or interacting elements.

- An *infrastructure* <organization> is a *system* of *facilities*, equipment and *services* needed for the operation of an *organization*.
  docue
- The *work environment* is a set of *conditions* under which work is performed.

- *Metrological confirmation* is a set of operations required to ensure that *measuring equipment* conforms to the *requirements* for its *intended use*. It generally includes calibration or verification, any necessary adjustment or *repair*, and subsequent recalibration, comparison with the metrological requirements for the intended use of the equipment, as well as any required sealing and labelling. It is not achieved until and unless the fitness of the *measuring equipment* for the *intended use* has been *demonstrated* and *documented*.

- The *measurement management system* is a set of interrelated or interacting elements necessary to achieve *metrological confirmation* and *control* of measurement *processes*.

- A *policy* <organization> is the intentions and direction of an *organization* as formally expressed by its *top management*.

- The *quality policy* is the *policy* related to *quality*. Generally, it is consistent with the overall *policy* of the *organization*, can be aligned with the *organization*'s *vision* and *mission* and provides a framework for the setting of *quality objectives*.

- The *vision* <organization> is the aspiration of what an *organization* would like to become as expressed by *top management*.

- The *mission* <organization> is the *organization*'s purpose for existing as expressed by *top management*.

- A *strategy* is a *plan* to achieve a long-term or overall *objective*.

- An *object* (*entity*, *item*) is anything perceivable or conceivable.

- *Quality* is the degree to which a set of inherent *characteristics* of an *object* fulfils *requirements*.

- A *grade* is a category or rank given to different *requirements* for an *object* having the same functional use.

- A *requirement* is a *need* or expectation that is stated, generally implied or obligatory. "*Generally implied*" means that it is custom or common practice for the

organization and *interested parties* that the need or expectation under consideration is implied.

- A *specified requirement* is one that is stated, for example in *documented information*. A qualifier can be used to denote a specific type of *requirement*, e.g. *product* requirement, *quality management* requirement, *customer* requirement, *quality* requirement. Requirements can be generated by different *interested parties* or by the *organization* itself. It can be necessary for achieving high customer satisfaction to fulfil an expectation of a customer even if it is neither stated nor generally implied or obligatory.

- A *quality requirement* is a *requirement* related to *quality*.

- A *statutory requirement* is an *obligatory requirement* specified by a legislative body.

- A *regulatory requirement* is an *obligatory requirement* specified by an authority mandated by a legislative body.

- *Product configuration information* is a *requirement* or other *information* for *product* design, realization, verification, operation and support.

- *Nonconformity* is non-fulfilment of a *requirement*.

- A *defect* is a *nonconformity* related to an intended or specified use. The distinction between the concepts *defect* and *nonconformity* is important as it has legal connotations, particularly those associated with *product* and *service* liability issues.
  The *intended use* as intended by the *customer* can be affected by the nature of the *information*, such as operating or maintenance instructions, provided by the *provider*.

- *Conformity* is fulfilment of a *requirement*.

- A *capability* is an ability of an *object* to realize an *output* that will fulfil the *requirements* for that *output*.

- *Traceability* is the ability to trace the history, application or location of an *object*.

- *Dependability* is the ability to perform as and when required.

- *Innovation* is new or changed *object* realizing or redistributing value.

- An *objective* is a result to be achieved.
  It can be strategic, tactical, or operational. It can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a quality objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

- A *quality objective* is an *objective* related to *quality*.
  These are generally based on the *organization*'s *quality policy* and are generally specified for relevant functions, levels and *processes* in the *organization*.
  In the context of quality management systems (3.5.4) *quality objectives* are set by the *organization*, consistent with its *quality policy*, to achieve specific results.

- *Success* <organization> is the achievement of an *objective*.

- The *success of an organization* emphasizes the need for a balance [35] between its economic or financial interests and the needs of its *interested parties*, such as *customers*, *users*, investors/shareholders (owners), people in the organization, *providers*, partners, interest groups and communities.

- *Sustained success* <organization> is *success* over a period of time.
  It emphasizes the need for a balance between economic-financial interests of an *organization* and those of the social and ecological environment. Sustained success relates to the *interested parties* of an *organization*.

- *Output* is the result of a *process*.

- A *product* is an *output* of an *organization* that can be produced without any transaction taking place between the *organization* and the *customer*.

- A *service* is *output* of an *organization* with at least one activity necessarily performed between the *organization* and the *customer*.

- *Performance* is a *measurable* result. It can relate either to quantitative or qualitative findings. It can relate to the *management* of *activities*, *processes*, *products*, *services*, *systems* or *organizations*.

- A *risk* is an effect of *uncertainty*. It is a deviation from the expected — positive or negative.

- *Uncertainty* is the state, even partial, of deficiency of *information* related to, understanding or knowledge of, an event, its *consequence*, or likelihood.

- *Efficiency* is a relationship between the result achieved and the resources used.

- *Effectiveness* is the extent to which planned *activities* are realized and planned results are achieved.

- *Data* is *facts* about an *object*.

[35] Balanced Scorecard

- *Information* is meaningful *data*.
- *Objective evidence* is *data* supporting the existence or verity of something. It can be obtained through observation, *measurement*, *test*, or by other means. Objective evidence for the purpose of *audit* generally consists of *records*, statements of fact or other *information* which are relevant to the *audit criteria* and *verifiable*.
- A *document* is *information* and the medium on which it is contained.
- *Documented information* is *information* required to be controlled and maintained by an *organization* and the medium on which it is contained.
- A *specification* is a *document* stating *requirements*.
- A *quality manual* is a *specification* for the *quality management system* of an *organization*.
- A *quality plan* is a *specification* of the *procedures* and associated resources to be applied when and by whom to a specific *object*. These procedures generally include those referring to *quality management processes* and to *product* and *service* realization *processes*. A *quality plan* often makes reference to parts of the *quality manual* or to procedure *documents*. A *quality plan* is generally one of the results of *quality planning*.
- A *record* is a *document* stating results achieved or providing evidence of activities performed. They can be used, for example, to formalize *traceability* and to provide evidence of *verification*, *preventive action* and *corrective action*.
- A *project management plan* is a *document* specifying what is necessary to meet the *objectives* of the *project*. It should include or refer to the project's *quality plan* and also includes or references such other plans as those relating to organizational structures, resources, schedule, budget, *risk management*, environmental management, health and safety management, and security management, as appropriate.
- *Verification* is the *confirmation*, through the provision of *objective evidence*, that specified *requirements* have been fulfilled. The *objective evidence* needed for a *verification* can be the result of an *inspection* or of other forms of *determination* such as performing alternative calculations or reviewing *documents*. The *activities* carried out for *verification* are sometimes called a *qualification process*.
- *Validation* is the *confirmation*, through the provision of *objective evidence*, that the *requirements* for a specific *intended use* or application have been fulfilled. The *objective evidence* needed for a *validation* is the result of a *test* or other form of *determination* such as performing alternative calculations or reviewing *documents*.
- A *characteristic* is a distinguishing feature.
- A *quality characteristic* is an inherent characteristic of an *object* related to a *requirement*.
- *Competence* is the ability to apply knowledge and skills to achieve intended results.
- *Metrological characteristic* is a *characteristic* which can influence the results of *measurement*.
- *Measuring equipment* usually has several *metrological characteristics*.
- A *configuration* is the set of interrelated functional and physical *characteristics* of a *product* or *service* defined in *product configuration information*.
- A *configuration baseline* is an approved *product configuration information* that establishes the *characteristics* of a *product* or *service* at a point in time that serves as reference for *activities* throughout the *life cycle* of the *product* or *service*.
- *Determination* is an *activity* to find out one or more *characteristics* and their characteristic values.
- *Review* is a *determination* of the *suitability*, *adequacy* or *effectiveness* of an *object* to achieve established *objectives*. It can also include the *determination* of *efficiency*.
- *Monitoring* is *determining* the status of a *system*, a *process*, a *product*, a *service*, or an *activity*. It is generally a *determination* of the status of an *object*, carried out at different *stages* or at different times.
- *Measurement* is a *process* to determine a value.
- A *measurement process* is a set of operations to determine the value of a quantity.
- An *inspection* is a *determination* of *conformity* to specified *requirements*. If the result of an *inspection* shows *conformity*, it can be used for purposes of *verification*. The result of an *inspection* can show *conformity* or *nonconformity* or a degree of *conformity*.
- *Test* is the *determination* according to *requirements* for a specific *intended use* or application. If the result of a test shows *conformity*, it can be used for purposes of *validation*.
- *Progress evaluation* <project management> is the assessment of progress made on achievement of the *project objectives*. This assessment should be carried out at appropriate points in the *project life cycle* across *project processes*, based on criteria for *project processes* and *product* or *service*. The results of *progress evaluations* can lead to revision of the *project management plan*.

- A *preventive action* is an action to eliminate the cause of a potential *nonconformity* or other potential undesirable situation. There can be more than one cause for a potential *nonconformity*. A *preventive action* is taken to prevent occurrence whereas *corrective action* is taken to prevent recurrence.

- A *corrective action* is an action to eliminate the cause of a *nonconformity* and to prevent recurrence.

- A *correction* is an action to eliminate a detected *nonconformity*.

- A *regrade* is the alteration of the *grade* of a *nonconforming product* or *service* in order to make it conform to *requirements* differing from the initial requirements.

- A *concession* is permission to use or *release* a *product* or *service* that does not conform to specified *requirements*. It is generally limited to the delivery of *products* and *services* that have *nonconforming characteristics* within specified limits and is generally given for a limited quantity of products and services or period of time, and for a specific use.

- A *deviation permit* is permission to depart from the originally specified *requirements* of a *product* or *service* prior to its realization.

- A *release* is permission to proceed to the next *stage* of a *process* or the next *process*.

- *Rework* is an action on a *nonconforming product* or *service* to make it conform to the *requirements*.

- *Repair* is an action on a *nonconforming product* or *service* to make it acceptable for the *intended use*. A successful *repair* of a *nonconforming product* or *service* does not necessarily make the *product* or *service* conform to the *requirements*. It can be that in conjunction with a *repair* a *concession* is required. Repair includes remedial action taken on a previously conforming *product* or *service* to restore it for use, for example as part of maintenance.

- *Scrap* is an action on a *nonconforming product* or *service* to preclude its originally *intended use*. In a nonconforming service situation, use is precluded by discontinuing the service.

- An *audit* is a systematic, independent and *documented process* for obtaining *objective evidence* and evaluating it objectively to determine the extent to which the *audit criteria* are fulfilled.
  The fundamental elements of an *audit* include the *determination* of the *conformity* of an *object* according to a *procedure* carried out by personnel not being responsible for the object audited.

- A *combined audit* is an *audit* carried out together at a single *auditee* on two or more *management systems*.

- A *joint audit* is an *audit* carried out at a single *auditee* by two or more *auditing organizations*.

- The *audit criteria* is a set of *policies*, *procedures* or *requirements* used as a reference against which *objective evidence* is compared.

- *Audit evidence* is *records*, statements of fact or other *information*, which are relevant to the *audit criteria* and verifiable.

- *Audit findings* is results of the evaluation of the collected *audit evidence* against *audit criteria*.

- *Audit conclusion* is the *outcome* of an *audit*, after consideration of the *audit objectives* and all *audit findings*.

21. Terms with respect to *Project, Programme, and Portfolio Management*

Source: [36]

…

- A *benefit* is a created advantage, value or other positive effect.
- A *business case* is a documented justification to support decision making about the commitment to a *project*, *programme* or *portfolio*.
- A *deliverable* is a unique and verifiable element that is required to be produced by a *project*.
- *Governance* is the *principles*, *policies* and framework by which an *organization* is *directed* and *controlled*.
- The *governing body* is the person, group or *entity accountable* for the *governance* of an *organization*, organizations, or a part of an organization.
- An *opportunity* is a *risk* occurrence that would have a favourable *impact*.
- An *outcome* is a change resulting from the use of the *output* from a project.
- An *output* is the set of aggregated tangible or intangible *deliverables* that form the *project* result.
- A *portfolio* is a collection of *portfolio components* grouped together to facilitate their *management* to meet strategic *objectives*.
- A *portfolio component* is a *project*, *programme*, *portfolio*, or other related work.
- *Portfolio management* is the set of coordinated *activities* to *direct* and *control* the accomplishment of strategic *objectives*.
- A *programme* is a group of *programme components* managed in a coordinated way to realize *benefits*.
- A *programme component* is a *project*, *programme* or other related work
- *Programme management* is the set of coordinated activities to *direct* and *control* the realisation of identified *benefits* and *deliverables*.
- A *project* is a temporary endeavour to achieve one or more defined *objectives*.
- *Project management* is the set of coordinated *activities* to *direct* and *control* the accomplishment of agreed *objectives*.
- A *sponsor* is a person responsible for obtaining the resources and executive decisions to enable *success*.
- A *stakeholder* is a person, group or *organization* that has interests in, or can affect, be affected by, or perceive itself to be affected by, any aspect of the *project*, *programme* or *portfolio*.
- A *threat* is a *risk* occurrence that would have a negative *impact*.

Source: [37]

- An *activity* is an identified *component of work* within a *schedule* that is required to be undertaken to complete a *project*.
- An *application area* is a category of *projects* that generally have a common focus related to a *product*, *customer* or sector.
- A *baseline* is a reference basis for comparison against which *project performance* is *monitored* and *controlled*.
- A *change request* is *documentation* that defines a proposed alteration to the *project*.
- *Configuration management* is the application of *procedures* to *control*, correlate and maintain *documentation*, *specifications* and physical attributes.
- *Control* is the comparison of actual *performance* with planned performance, analysing variances and taking appropriate *corrective actions* and *preventive actions* as needed.
- A *corrective action* is *direction* and *activity* for modifying the *performance* of work to bring *performance* in line with the *plan*.
- The *critical path* is the sequence of *activities* that determine the earliest possible completion date for the *project* or *phase*.
- *Lag* is an attribute applied to a logical relationship to delay the start or end of an *activity*.
- *Lead* is an attribute applied to a logical relationship to advance the start or end of an *activity*.

[36] ISO/DIS 21500 *Project, programme and portfolio management -- Context and concepts*
[37] ISO 21500:2012 *Guidance on project management*

- A *preventive action* is *direction* and *activity* for modifying the work, in order to avoid or reduce potential *deviations* in *performance* from the *plan*.
- A *project life cycle* is a defined set of *phases* from the start to the end of the *project*.
- A *risk register* is a *record* of identified *risks*, including results of analysis and planned responses.
- A *stakeholder* is a person, group or *organization* that has interests in, or can affect, be affected by, or perceive itself to be affected by, any aspect of the *project*.
- A *tender* is a *document* in the form of an offer or statement of bid to supply a *product*, *service* or result, usually in response to an invitation or request.
- A *work breakdown structure dictionary* is a *document* that describes each component in the *work breakdown*.

Source: [38]

- The *100% rule* is a concept concerning the entire *work* required to be accomplished to achieve a *project* or *programme* scope captured in the *work breakdown structure*.
- An *activity* is identified piece of work that is required to be undertaken to complete a *project* or *programme*.
- *Actual cost* is the cost incurred for work performed.
- A *benefit* is a created advantage, value or other positive effect.
- The *budget at completion* is the total forecasted cost for accomplishing the work related to a *work package*, *activity* or *control account*.
- A *business case* is the documented justification to support decision making about the commitment to a *project*, *programme* or *portfolio*.
- A *change register* is a *record* of all identified *project* changes and their attributes.
- A *change request* is *documentation* that defines a proposed alteration to a *project*.
- A *communication plan* is a documented description and communication needs of *stakeholders*.
- *Configuration management* is an application of *procedures* to *control*, correlate and maintain *documentation*, *specifications* and physical attributes.
- *Control* is comparison of actual *performance* with planned performance, analysing variances and taking appropriate *corrective action* and *preventive action* as needed.
- A *control account* is a management *control point* where scope, budget, *actual cost* and schedule of a *project* or *programme*, *work package* or *activity* are integrated.
- A *corrective action* is direction and *activity* for modifying the *performance* of work to bring *performance* in line with a *plan*.
- A *cost variance* is a measure of cost performance on a *project*.
- *Crashing* is a schedule compression technique to shorten the duration of an *activity*, a group of activities or a *project* by increasing the expenditure of resources.
- A *critical path* is a sequence of *activities* that determine the earliest possible completion date for a *project* or *phase*.
- A *deliverable* is a unique and verifiable, tangible or intangible outcome of a planned *activity*.
- The *earned value* is the budgeted cost of work performed value of completed work expressed in terms of the budget assigned to that work.
- *Earned value management* (EVM) is a method that integrates *project* or *programme* scope, *actual cost*, budget and schedule for *assessment* of *progress* and *performance*.
- The *estimate at completion* is a forecasted total cost to accomplish the work on a *project*, *programme*, *work package* or *activity*.
- The *estimate to complete* is a forecasted cost of the work remaining on a *project*, *programme*, *work package* or *activity*.
- A *functional breakdown structure* is a decomposition of the functions necessary to perform the work elements of a *project* or *programme*.
- *Governance* is the *principles*, *policies* and *framework* by which an *organization* is *directed* and *controlled*.
- The *governing body* is the person, group or *entity accountable* for the *governance* of an *organization*, organizations or a part of an organization.
- An *integrated baseline review* is an *assessment* to establish a common understanding of the *performance*

[38] ISO/TR 21506:2018 *Project, programme and portfolio management — Vocabulary*

measurement baseline for *verification* of the technical content of a *project* or *programme*.

- *Lag* is an attribute applied to a logical relationship to delay the start or end of an *activity*.
- *Lead* is an attribute applied to a logical relationship to advance the start or end of an *activity*.
- *Lessons learned* is knowledge gained throughout a *project*, *programme* or *portfolio* that shows how events were addressed or should be addressed for the purpose of improving future performance.
- A *make-or-buy decision* is the *determination* to internally produce a *product*, *work* or *service* in-house or to purchase it from an outside source.
- A *management information system* is hardware and software used to support the compilation of *information*, analysis and reporting of *project* and *programme* metrics.
- The *management reserve* is the amount of budget external to a *performance measurement baseline*, withheld for management control in response to unforeseen events or activities that are a part of the scope.
- A *milestone* is a significant planned, or to be planned, point in a *project*, *programme* or *portfolio*.
- A *network schedule* is a graphical representation indicating the logic sequencing and interdependencies of the work elements of a *project* or *programme*.
- An *opportunity* is a *risk* occurrence that would have a favourable *impact*.
- An *organizational breakdown structure* is a decomposition of the management team of an *organization* or of the management team that performs the work of a *project* or *programme*.
- The *organizational breakdown structure* can include partnering or subcontracting. It is used to illustrate the relationship between *project* and *programme activities* and the organizational units that will manage or perform the work *activities*.
- *Performance measurement* is the quantitative units of measure that are placed to track progress.
- The *performance measurement baseline* is the total time-phased scope of work and budget plan against which *project* or *programme performance* is measured, not including *management reserve*.
- The *planned value* (budgeted cost of work scheduled) is the *time-phased budget* authorized for the work scheduled.
- A *portfolio* is a collection of *portfolio components* grouped together to facilitate their *management* to meet strategic *objectives*.
- A *portfolio component* is a *project*, *programme*, *portfolio* or other related work.
- *Portfolio governance* is the *principles*, *policies* and *procedures* by which a *portfolio* is authorized and directed to meet strategic *objectives*.
- *Portfolio management* is the set of coordinated *activities* to *direct* and *control* the accomplishment of strategic *objectives*.
- A *portfolio manager* is person appointed with the *accountability* and *responsibility* for a *portfolio* to meet strategic *objectives*.
- A *portfolio plan* is a documented description of a *portfolio*'s alignment to strategic *objectives* and *integrated management baselines*.
- A *portfolio pipeline* is the collection of *opportunities* considered for selection as *portfolio components*.
- A *product breakdown structure* is a decomposition of a *product* into its components.
- A *programme* is a group of *programme components* managed in a coordinated way to realize *benefits*.
- A *programme benefit* is an assessable *outcome* viewed as an advantage by programme *stakeholders* and contributing to the programme *objectives*.
- A *programme component* is a *project*, *programme* or other related work.
- *Programme governance* is the *principles*, *policies* and *procedures* by which a *programme* is authorized and directed to realize identified *benefits*.
- *Programme management* is the coordinated *activities* to direct and control the realization of identified *benefits* and *deliverables*.
- A *programme manager* is a person appointed with the *accountability* and *responsibility* of a *programme* to realize identified *benefits* and *deliverables*.
- A *programme plan* is the documented description of the *integrated technical and management baselines* to be followed for a *programme*.
- A *progress report* is a *report* of current status and work accomplished during a specified time period.
- A *progressive elaboration* (*progressive decomposition*) is an iterative *process* to incorporate an increased level of detail as identified during the *life cycle* of a *project* or programme.

- A *project* is temporary endeavour created to produce agreed *deliverables*.
- *Project governance* is the *principles*, *policies* and *procedures* by which a project is authorized and directed to accomplish agreed *deliverables*.
- *Project management* is the coordinated *activities* to *direct* and *control* the accomplishment of agreed *deliverables*.
- A *project management office* is a function or organizational structure facilitating the management of *projects*.
- A *project manager* is a person appointed to lead a *project* team and to be *accountable* and *responsible* for a project's agreed *deliverables*.
- A *project plan* is documented description of the *technical and management baselines* to be followed for a *project*.
- The *project scope* is *authorized work* to accomplish agreed *deliverables*.
- A *project scope statement* is a documented detailed description of a *project scope*.
- *Quality assurance* is the planned and systematic actions necessary to provide adequate confidence that a *process*, *measurement* or *service* satisfies given *requirements for quality*.
- *Quality control* is the *assessment* of specific results to *determine conformity* with relevant standards and to identify steps to eliminate unsatisfactory performance.
- *Quality plan* is the documented description of *quality requirements* for interim and final *deliverables*.
- A *resource breakdown structure* is a decomposition of personnel, equipment, material or other assets.
- A *responsibility assignment matrix* is a documented structure that shows the allocation of delegated work responsibilities designated for the delivery of a *scope* or *benefits*.
- A *risk* is an *uncertain event* or set of events with a potential positive or negative *impact*.
- A *risk breakdown structure* is a decomposition of *threats* and *opportunities* for a *project* or *programme*.
- A *risk response* is a documented action in regard to an identified *risk*.
- The *risk tolerance* is an assessed and accepted threshold levels of *risk* exposure that when exceeded will trigger a *risk response*.
- *Rolling wave planning* is a form of *progressive elaboration* where planning is accomplished in *phases* or time periods.
- *Scope creep* is the unauthorized and uncontrolled increases to *project scope*.
- A *sponsor* is a person responsible for obtaining the resources and executive decisions to enable success.
- A *stakeholder* is a person, group or *organization* that has interests in, or can affect, be affected by, or perceive itself to be affected by, any aspect of a *project*, *programme* or *portfolio*.
- A *stakeholder register* is a *record* of identified *stakeholders* and their attributes.
- *Strategic alignment* is a linkage of *portfolio objectives* and components with *strategy*.
- *Technical performance* is a *measure* of the results of functionalities or capabilities achieved for a *project* or *programme* during implementation.
- A *threat* is a *risk* occurrence that would have a negative impact.
- A *time-phased budget* is the allocation of the cost to accomplish work over established periods of time or *phases*.
- The *undistributed budget* is the cost for *authorized work* that has not been distributed to a *control account*.
- The *variance at completion* is the difference between *budget at completion* and *estimate at completion*.
- A *work breakdown structure* is a decomposition of the defined *scope of a project* or *programme* into progressively lower levels consisting of elements of work.
- A *work breakdown structure dictionary* is a *document* that describes each element in a *work breakdown structure*.
- A *work breakdown structure element* is work at a designated level that is either a *parent element* or a *child element*.
- A *work package* is one or more groups of related *activities* that are within a *control account*.

22. Terms with respect to *Safety*

Source: [39]

The term "*safe*" is often understood by the general public as the state of being protected from all hazards. However, this is a misunderstanding: "*safe*" is rather the state of being protected from recognized hazards that are likely to cause harm. Some level of risk is inherent in products or systems.

- *Harm* is injury or damage to the health of people, or damage to property or the environment.
- A *hazard* is a potential source of *harm*.
- A *hazardous event* is an *event* that can cause *harm*.
- A *hazardous situation* is a circumstance in which people, property or the environment is/are exposed to one or more *hazards*.
- An *inherently safe design* is *measures* taken to eliminate *hazards* and/or to reduce *risks* by changing the design or operating *characteristics* of the *product* or *system*.
- The *intended use* is the *use* in accordance with *information* provided with a *product* or *system*, or, in the absence of such information, by generally understood *patterns* of usage.
- A *reasonably foreseeable misuse* is the *use* of a *product* or *system* in a way not intended by the *supplier*, but which can result from readily predictable human behaviour. Readily predictable human behaviour includes the behaviour of all types of users, e.g. the elderly, children and persons with disabilities. In the context of consumer safety, the term *reasonably foreseeable use* is increasingly used as a synonym for both *intended use* and *reasonably foreseeable misuse*.
- *Residual risk* is the *risk* remaining after *risk reduction measures* have been implemented.
- A *risk* is a combination of the *probability* of occurrence of *harm* and the *severity* of that harm. The *probability* of occurrence includes the exposure to a *hazardous situation*, the occurrence of a *hazardous event* and the possibility to avoid or limit the harm.
- A *risk analysis* is the systematic use of available *information* to identify *hazards* and to estimate the *risk*.
- A *risk assessment* is an overall *process* comprising a *risk analysis* and a *risk evaluation*.
- A *risk evaluation* is a *procedure* based on the *risk analysis* to determine whether *tolerable risk* has been exceeded.
- A *risk reduction measure* (*protective measure*) is an action or means to eliminate *hazards* or reduce *risks*.
- *Safety* is the freedom from *risk* which is not *tolerable*.
- *Tolerable risk* is the level of *risk* that is accepted in a given context based on the current values of society.
- A *vulnerable consumer* is a *consumer* at greater *risk* of *harm* from *products* or *systems*, due to age, level of literacy, physical or mental condition or limitations, or inability to access product *safety information*.

[39] ISO/IEC Guide 51:2014 *Safety aspects — Guidelines for their inclusion in standards*

23. Terms with respect to *Security and Resilience*

Source: [40]

...

- An *activity* is a *process* or set of processes undertaken by an *organization* (or on its behalf) that produces or supports one or more *products* or *services*.
- An *asset* is anything that has *value* to an *organization*.
- An *attack* is a successful or unsuccessful attempt(s) to circumvent an authentication solution, including attempts to imitate, produce or reproduce the authentication elements.
- An *audit* is a systematic, independent and documented *process* for obtaining *audit evidence* and evaluating it objectively to determine the extent to which the *audit criteria* are fulfilled. The fundamental elements of an audit include the determination of the *conformity* of an *object* according to a *procedure* carried out by *personnel* not being responsible for the *object* audited.
- An *auditor* is a person who conducts an *audit*.
- *Authentic material good* is *material good* produced under the control of the legitimate manufacturer, originator of the goods or rights holder.
- *Authentication* is the *process* of corroborating an *entity* or *attributes* with a specified or understood level of *assurance*.
- An *authentication element* is a tangible *object*, visual *feature* or *information* associated with a *material good* or its packaging that is used as part of an *authentication solution*.
- An *authentication function* is a function performing *authentication*.
- An *authentication solution* is a complete set of means and *procedures* that allows the *authentication* of a *material good* to be performed.
- An *authentication tool* is a set of hardware and/or *software system*(s) that is part of an anti-counterfeiting solution and is used to control the *authentication element*.
- An *authoritative source* is an official origination of an *attribute* which is also responsible for maintaining that *attribute*.
- *Automated interpretation* is a *process* that automatically evaluates *authenticity* by one or more components of the *authentication solution*.
- *Business continuity* is the *capability* of an *organization* to continue the delivery of *products* or *services* at acceptable predefined levels following a *disruption*.
- *Business continuity management* is a holistic *management process* that identifies potential *threats* to an *organization* and the *impact* those *threats*, if realized, can cause on *business operations*, and provides a *framework* for building *organizational resilience* with the *capability* of an *effective response* that safeguards the interests of key *interested parties*, reputation, brand and value-creating *activities*.
- A *business continuity management system* is part of the overall *management system* that establishes, implements, operates, monitors, reviews, maintains and improves *business continuity*. Such a management system includes organizational structure, *policies*, *planning*, *activities*, responsibilities, *procedures*, *processes* and *resources*.
- A *business continuity plan* is a set of documented *procedures* that guide an *organization* to respond, recover, resume and restore itself to a pre-defined level of operation following a *disruption*. Typically, this covers *resources*, *services* and *activities* required to ensure the *continuity* of *critical business functions*.
- A *business continuity programme* is an ongoing *management* and *governance process* supported by *top management* and appropriately resourced to implement and maintain *business continuity management*.
- A *business impact analysis* is a *process* of analysing *activities* and the effect that a business *disruption* can have upon them.
- *Capacity* is the combination of all the strengths and *resources* available within an *organization*, *community* or society that can reduce the *level of risk* or the effects of a *crisis*. It can include physical, institutional, social, or economic means as well as skilled *personnel* or *attributes* such as leadership and *management*.
- *Command and control* is a set of *activities* of target-orientated decision making, including assessing the situation, planning, implementing decisions and controlling the effects of implementation on the *incident*. This *process* is continuously repeated.
- A *command and control system* is a *system* that supports *effective emergency management* of all available *assets* in a preparation, *incident response*, *continuity* and/or *recovery process*.

[40] ISO 22300:2018 *Security and resilience — Vocabulary*

- A *community* is a group of associated *organizations*, individuals and groups sharing common interests.
- A *contingency* is a possible future *event*, *condition* or eventuality.
- *Continuity* is the strategic and tactical *capability*, pre-approved by *management*, of an *organization* to *plan* for and *respond* to *conditions*, situations and *events* in order to continue operations at an acceptable predefined level. It is the more general term for operational and business continuity to ensure an *organization*'s ability to continue operating outside of normal *operating conditions*.
- *Cooperation* is the *process* of working or acting together for common interests and *values* based on *agreement*.
- *Coordination* is the way in which different *organizations* (public or private) or parts of the same *organization* work or act together in order to achieve a common *objective*.
- *Countermeasure* is an action taken to lower the *likelihood* of a security *threat scenario* succeeding in its *objectives*, or to reduce the likely *consequences* of a security *threat scenario*.
- A *crisis* is an unstable *condition* involving an impending abrupt or significant change that requires urgent attention and action to protect life, *assets*, property or the *environment*.
- *Crisis management* is a holistic *management process* that identifies potential *impacts* that threaten an *organization* and provides a framework for building *resilience*, with the *capability* for an *effective response* that safeguards the interests of the *organization*'s key *interested parties*, reputation, brand and value-creating *activities*, as well as effectively restoring operational *capabilities*. It also involves the management of preparedness, mitigation, response, and continuity or recovery in the event of an incident, as well as management of the overall programme through training, rehearsals and reviews to ensure the preparedness, response and continuity plans stay current and up-to-date.
- *Critical control point* is a point, step or *process* at which *controls* can be applied and a *threat* or *hazard* can be prevented, eliminated or *reduced* to *acceptable levels*.
- A *critical customer* is an *entity*, the loss of whose business would threaten the survival of an *organization*.
- A *critical product* or *service* is a *resource* obtained from a *supplier* which, if unavailable, would *disrupt* an *organization*'s *critical activities* and threaten its survival. These are essential *resources* to support an *organization*'s high priority activities and processes identified in its *business impact analysis*.
- A *critical supplier* is a *provider* of *critical products or services*. This includes an "internal supplier", who is part of the same organization as its customer.
- A *criticality analysis* is a *process* designed to systematically identify and evaluate an *organization*'s *assets* based on the importance of its *mission* or function, the group of people at risk, or the significance of an *undesirable event* or *disruption* on its *ability* to meet expectations.
- *Custody* is the period of time where an *organization* in the *supply chain* is directly controlling the manufacturing, handling, processing and transportation of *goods* and their related shipping *information* within the *supply chain*.
- A *disaster* is a situation where widespread human, material, economic or environmental losses have occurred which exceeded the ability of the affected *organization*, *community* or society to respond and recover using its own *resources*.
- A *disruption* is an *event*, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of *products* or *services* according to an *organization*'s *objectives*.
- *Downstream* is the handling, processing and movement of *goods* when they are no longer in the *custody* of the *organization* in the *supply chain*.
- An *emergency* is a sudden, urgent, usually unexpected occurrence or *event* requiring immediate action. It is usually a *disruption* or *condition* that can often be anticipated or prepared for, but seldom exactly foreseen.
- An *entity* is something that has a separate and distinct existence and that can be identified within context.
- An *evaluation* is a systematic *process* that compares the result of *measurement* to recognised *criteria* to determine the discrepancies between intended and actual performance. Gaps in performance are inputs into the *continual improvement process*.
- An *exercise* is a *process* to train for, assess, practise and improve *performance* in an *organization*.
- An *exercise programme* is a series of *exercise activities* designed to meet an overall *objective* or goal.
- The *exercise programme manager* is the person responsible for planning and improving the *exercise programme*.
- The *exercise project team* is a group of individuals responsible for planning, conducting and evaluating an exercise project.
- The *false acceptance rate* is the proportion of *authentications* wrongly declared true.

- The *false rejection rate* is the proportion of *authentications* wrongly declared false.
- A *functional exercise* is an *exercise* to train for, assess, practise and improve the *performance* of single functions designed to respond to and recover from an unwanted *event*.
- *Goods* are *items* or materials that, upon the placement of a purchase order, are manufactured, handled, processed or transported within the *supply chain* for usage or consumption by the purchaser.
- A *hazard monitoring function* is a set of *activities* to obtain evidence-based *information* on *hazards* in a defined area used to make decisions about the need for public warning.
- *Identification* is the *process* of recognizing the *attributes* that *identify* an *entity*.
- An *identifier* is a specified set of *attributes* assigned to an *entity* for the purpose of *identification*.
- An *identity* is a set of *attributes* that are related to an *entity*.
- *Impact* is the evaluated *consequence* of a particular *outcome*.
- *Impact analysis* (*consequence analysis*) is a *process* of analysing all operational functions and the effect that an operational interruption can have upon them. It is part of the *risk assessment process* and includes *business impact analysis*.
- *Impartiality* is the actual or perceived presence of *objectivity*. Objectivity means that conflicts of interest do not exist or are resolved so as not to adversely influence subsequent activities.
- An *incident* is a situation that can be, or could lead to, a *disruption*, loss, *emergency* or *crisis*.
- *Incident command* is a *process* that is conducted as part of an *incident management system*, and which evolves during the *management* of an *incident*.
- An *incident management system* is a *system* that defines the roles and responsibilities of *personnel* and the operating *procedures* to be used in the *management* of *incidents*.
- *Incident preparedness* is the set of *activities* taken to prepare for *incident response*.
- *Incident response* is the set of *actions* taken in order to stop the causes of an imminent *hazard* and/or *mitigate* the *consequences* of potentially destabilizing *events* or *disruptions*, and to *recover* to a normal situation.
- *Information* is *data* processed, organized and correlated to produce meaning.
- An *inherently dangerous property* is a *property* that, if in the hands of an unauthorized individual, would create an imminent *threat* of death or serious bodily *harm*.
- An *inject* is a scripted piece of *information* inserted into an *exercise* that is designed to elicit a *response* or decision and facilitate the flow of the *exercise*.
- *Integrity* is the *property* of safeguarding the accuracy and completeness of *assets*.
- An *international supply chain* is a *supply chain* that at some point crosses an international or economic border.
- *Interoperability* is the *ability* of diverse *systems* and *organizations* to work together.
- A *key performance indicator* (KPI) is a quantifiable measure that an *organization* uses to gauge or compare *performance* in terms of meeting its strategic and operational *objectives*.
- A *logical structure* is an arrangement of *data* to optimize their access or processing by given *user* (human or machine).
- A *management plan* is a clearly defined and documented *plan* of action, typically covering the key *personnel*, *resources*, *services*, and actions needed to implement the *management process*.
- *Mitigation* is the limitation of any negative *consequence* of a particular *incident*.
- An *object* is a single and distinct *entity* that can be *identified*.
- An *observer* is a *participant* who witnesses the *exercise* while remaining separate from *exercise activities*.
- *Operational information* is *information* that has been contextualized and analysed to provide an understanding of the situation and its possible evolution.
- An *owner* is an *entity* that legally controls the licensing and user rights and distribution of the object associated with the unique identifier.)
- A *participant* is a person or *organization* who performs a function related to an *exercise*.
- *Partnering* is *associating* with others in an *activity* or area of common interest in order to achieve individual and collective *objectives*.
- *People at risk* are the individuals in the area who may be affected by an *incident*.

- A *performance evaluation* is a *process* of determining *measurable* results.
- *Personnel* is the people working for and under the control of an *organization*.
- *Planning* is part of *management* focused on setting *objectives* and specifying necessary operational *processes* and related *resources* to fulfil those *objectives*.
- *Preparedness* (*readiness*) is the set of *activities*, *programmes*, and *systems* developed and implemented prior to an *incident* that can be used to support and enhance *prevention*, *protection* from, *mitigation* of, *response* to and *recovery* from *disruptions*, *emergencies* or *disasters*.
- *Prevention* is the measures that enable an *organization* to avoid, preclude or limit the *impact* of an *undesirable event* or potential *disruption*.
- *Prevention of hazards and threats* is the *process*, practices, techniques, materials, *products*, *services* or *resources* used to avoid, reduce, or control *hazards* and *threats* and their associated *risks* of any type in order to reduce their potential *likelihood* or *consequences*.
- A *prioritized activity* is an *activity* to which priority is given following an *incident* in order to *mitigate impacts*.
- A *product* or *service* is a *beneficial outcome* provided by an *organization* to its *customers*, recipients and *interested parties*.
- *Protection* is the measures that safeguard and enable an *organization* to reduce the *impact* of a potential *disruption*.
- *Recovery* is the restoration and *improvement*, where appropriate, of *operations*, *facilities*, livelihoods or living *conditions* of affected *organizations*, including efforts to reduce *risk* factors.
- *Resilience* is the *ability* to absorb and adapt in a changing *environment*.
- A *resource* is an *asset*, *facility*, equipment, material, *product* or waste that has potential *value* and can be used.
- A *response plan* is a documented collection of *procedures* and *information* that is developed, compiled and maintained in *readiness* for use in an *incident*.
- A *response programme* is the *plan*, *processes*, and *resources* to perform the *activities* and *services* necessary to preserve and protect life, property, operations and critical *assets*.
- *Risk appetite* is the amount and type of *risk* that an *organization* is willing to pursue or retain.
- *Risk communication* is the exchange or sharing of *information* about *risk* between the decision maker and other *interested parties*.
- *Risk identification* is a *process* of finding, recognizing and describing *risks*. It involves the identification of risk *sources*, *events*, their causes and their potential *consequences*.
- *Risk management* is the coordinated *activities* to direct and control an *organization* with regard to *risk*. It generally includes *risk assessment*, *risk treatment*, *risk acceptance*, and *risk communication*.
- *Risk reduction* is actions taken to lessen the *probability* or negative *consequences*, or both, associated with a *risk*.
- *Robustness* is the *ability* of a *system* to resist virtual or physical, internal or external attacks.
- A *scenario* is a pre-planned storyline that drives an *exercise*, as well as the stimuli used to achieve *exercise project performance objectives*.
- A *script* is a story of the *exercise* as it develops which allows directing staff to understand how *events* should develop during *exercise* play as the various elements of the master *events* list are introduced. It is often written as a narrative of simulated *events*.
- A *secret* is *data* and/or *knowledge* that are *protected* against disclosure to unauthorised *entities*.
- *Security* is the state of being free from danger or *threat*.
- A *security aspect* is a *characteristic*, element, or *property* that reduces the *risk* of unintentionally-, intentionally-, and naturally-caused *crises* and *disasters* which *disrupt* and have *consequences* on the *products* or *services*, *operation*, *critical assets* and *continuity* of an *organization* and its *interested parties*.
- *Semantic interoperability* is the *ability* of two or more *systems* or *services* to automatically interpret and use *information* that has been exchanged accurately.
- *Sensitive information* is *information* that is *protected* from public disclosure only because it would have an *adverse* effect on an *organization*, national security or public safety.
- *Subcontracting* is *contracting* with an *external party* to fulfil an obligation arising out of an existing contract.
- *Syntactic interoperability* is the *ability* of two or more *systems* or *services* to exchange structured *information*.
- A *target* is a detailed *performance requirement*, applicable to an *organization* or parts thereof, that arises

from the *objectives* and that needs to be set and met in order to achieve those *objectives*.

- A *test* is a unique and particular type of *exercise*, which incorporates an expectation of a pass or fail element within the aim or *objectives* of the *exercise* being planned.

- *Testing* is a *procedure* for *evaluation*; a means of *determining* the presence, quality or veracity of something.

- A *threat* is a potential cause of an *unwanted incident*, which may result in *harm* to individuals, *assets*, a *system* or *organization*, the *environment* or the *community*.

- *Threat analysis* is a *process* of identifying, qualifying and quantifying the potential cause of an *unwanted event*, which may result in *harm* to individuals, *assets*, a *system* or *organization*, the *environment*, or the *community*.

- A *tier 1 supplier* is a *provider* of *products* or *services* directly to an *organization* usually through a contractual arrangement.

- A *tier 2 supplier* is a *provider* of *products* or *services* indirectly to an organization through a *tier 1 supplier*.

- *Training* is the *activities* designed to facilitate the learning and development of *knowledge*, *skills* and *abilities*, and to *improve* the *performance* of specific *tasks* or roles.

- An *undesirable event* is an occurrence or *change* that has the potential to cause loss of life, *harm* to tangible or intangible *assets*, or negatively *impact* the human rights and fundamental freedoms of internal or external *interested parties*.

- *Upstream* is the handling, processing and movement of goods that occurs before the *organization* in the *supply chain* takes *custody* of the *goods*.

- A *vulnerability analysis* (*vulnerability assessment*) is a *process* of identifying and quantifying something that creates susceptibility to a *source* of *risk* that can lead to a *consequence*.

24. Terms with respect to *Information Security*

Source: [41]

...

- *Access control* is a means to ensure that access to assets is authorized and restricted based on business and security *requirements*.
- An *attack* is an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an *asset*.
- The *audit scope* is the extent and boundaries of an *audit*.
- *Authentication* is the provision of *assurance* that a claimed *characteristic* of an *entity* is correct.
- A *base measure* is a *measure* defined in terms of an *attribute* and the method for quantifying it. It is functionally independent of other measures.
- A *control objective* is a statement describing what is to be achieved as a result of implementing *controls*.
- A *derived measure* is a *measure* that is defined as a function of two or more *values* of *base measures*.
- The *governance of information security* is the *system* by which an *organization*'s *information security* activities are directed and controlled.
- A *governing body* is a person or group of people who are accountable for the *performance* and *conformity* of the *organization*.
- An *indicator* is a *measure* that provides an estimate or evaluation.
- *Information need* is the insight necessary to manage *objectives*, goals, *risks* and problems.
- The *information processing facilities* are any information processing *system*, *service* or *infrastructure*, or the physical location housing it.
- *Information security* is the preservation of *confidentiality*, *integrity* and *availability* of *information*. In addition, other properties, such as *authenticity*, *accountability*, *non-repudiation*, and *reliability* can also be involved.
- *Information security continuity* is the *processes* and *procedures* for ensuring continued *information security* operations.
- An *information security event* is an identified occurrence of a *system*, *service* or network *state* indicating a possible breach of *information security policy* or failure of *controls*, or a previously unknown situation that can be security relevant.
- An *information security incident* is a single or a series of unwanted or unexpected *information security events* that have a significant probability of compromising business operations and threatening *information security*.
- *Information security incident management* is a set of *processes* for detecting, reporting, assessing, responding to, dealing with, and learning from *information security incidents*.
- An *information security management system* (ISMS) *professional* is a person who establishes, implements, maintains and continuously improves one or more *information security management system processes*.
- An *information sharing community* is a group of *organizations* that agree to share *information*.
- An *information system* is a set of *applications*, *services*, information technology *assets*, or other information-handling components.
- A *measure* is a variable to which a *value* is assigned as the result of *measurement*.
- *Measurement* is a *process* to determine a *value*.
- A *measurement function* is an algorithm or calculation performed to combine two or more *base measures*.
- A *measurement method* is a logical sequence of operations, described generically, used in quantifying an *attribute* with respect to a specified scale.
- *Non-repudiation* is the *ability* to prove the occurrence of a claimed *event* or action and its originating *entities*.
- The *review object* is the specific *item* being reviewed.
- A *review objective* is a statement describing what is to be achieved as a result of a *review*.
- A *security implementation standard* is document specifying authorized ways for realizing security.
- A *threat* is a potential cause of an unwanted incident, which can result in harm to a system or organization.

[41] ISO/IEC 27000:2018 *Information technology — Security techniques — Information security management syst. — Overview and vocabulary*

25. Terms with respect to *Privacy*

Source: [42]

...

- *Anonymity* is the *characteristic* of *information* that does not permit a PII *principal* to be identified directly or indirectly.
- *Anonymization* is a *process* by which *personally identifiable information* is irreversibly altered in such a way that a PII *principal* can no longer be identified directly or indirectly, either by the PII *controller* alone or in collaboration with any other *party*.
- *Anonymized data* is *data* that has been produced as the *output* of a *personally identifiable information anonymization process*.
- *Consent* is the PII *principal*'s freely given, specific and informed *agreement* to the *processing* of their PII.
- *Identifiability* is a *condition* which results in a PII *principal* being identified, directly or indirectly, on the basis of a given set of PII.
- To *identify* is to establish the link between a PII *principal* and PII or a set of PII.
- *Identity* is a set of *attributes* which make it possible to *identify* the PII *principal*.
- *Opt-in* is a *process* or type of *policy* whereby the PII *principal* is required to take an action to express explicit, prior *consent* for their PII to be processed for a particular *purpose*.
- *Personally identifiable information* (PII) is any *information* that (a.) can be used to *identify* the PII *principal* to whom such *information* relates, or (b.) is or might be directly or indirectly linked to a PII *principal*. To determine whether a PII *principal* is identifiable, account should be taken of all the means which can reasonably be used by the *privacy stakeholder* holding the *data*, or by any other *party*, to *identify* that natural person.
- A PII *controller* is a *privacy stakeholder* (or *privacy stakeholders*) that determines the purposes and means for processing *personally identifiable information* other than natural persons who use data for personal purposes. A PII *controller* sometimes instructs others (e.g., PII *processors*) to process PII on its behalf while the responsibility for the processing remains with the PII *controller*.
- A PII *principal* is a natural person to whom the *personally identifiable information* relates.
- A PII *processor* is a *privacy stakeholder* that processes *personally identifiable information* on behalf of and in accordance with the instructions of a PII *controller*.
- A *privacy breach* is a situation where *personally identifiable information* is processed in violation of one or more relevant privacy safeguarding requirements.
- *Privacy controls* is the *measures* that treat *privacy risks* by reducing their *likelihood* or their *consequences*. Such privacy controls include organizational, physical and technical measures, e.g., policies, procedures, guidelines, legal contracts, management practices or organizational structures.
- *Privacy enhancing technology* (PET) is *privacy control*, consisting of information and communication technology (ICT) *measures*, *products*, or *services* that protect *privacy* by eliminating or reducing PII or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system. Examples of PETs include, but are not limited to, *anonymization* and *pseudonymization* tools that eliminate, reduce, mask, or de-identify PII or that prevent unnecessary, unauthorized and/or undesirable processing of PII.
- The *privacy policy* is overall intention and direction, rules and commitment, as formally expressed by the PII *controller* related to the processing of PII in a particular setting.
- The *privacy preferences* is the set of specific choices made by a PII *principal* about how their PII should be processed for a particular purpose.
- The *privacy principles* is a set of shared values governing the privacy protection of PII when processed in ICT systems.
- *Privacy risk* is the effect of *uncertainty* on *privacy*.
- A *privacy risk assessment* is an overall *process* of *risk identification*, *risk analysis* and *risk evaluation* with regard to the processing of PII. This process is also known as a *privacy impact assessment*.
- *Privacy safeguarding requirements* is the set of *requirements* an *organization* has to take into account when processing PII with respect to the privacy protection of its PII.
- A *privacy stakeholder* is a natural or legal person, public authority, agency or any other body that can affect, be affected by, or perceive themselves to be affected by a

[42] ISO/IEC 29100:2011 *Information technology — Security techniques — Privacy framework*

decision or activity related to *personally identifiable information* (PII) processing.

- *Processing of* PII is the operation or set of operations performed upon *personally identifiable information* (PII). Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, *anonymization*, *pseudonymization*, dissemination or otherwise making available, deletion or destruction of PII.

- *Pseudonymization* is a *process* applied to *personally identifiable information* which replaces *identifying information* with an alias. It can be performed either by PII *principals* themselves or by PII *controllers*. It can be used by PII *principals* to consistently use a *resource* or *service* without disclosing their *identity* to this *resource* or *service* (or between services), while still being held accountable for that use.

- *Secondary use* is the processing of *personally identifiable information* in *conditions* which differ from the initial ones. Conditions that differ from the initial ones could involve, for example, a new *purpose* for processing PII, a new recipient of the PII, etc.

- *Sensitive* PII is the category of PII, either whose nature is sensitive, such as those that relate to the PII principal's most intimate sphere, or that might have a significant *impact* on the PII *principal*. In some jurisdictions or in specific contexts, *sensitive* PII is defined in reference to the nature of the PII and can consist of PII revealing the racial origin, political opinions or religious or other beliefs, personal data on health, sex life or criminal convictions, as well as other PII that might be defined as sensitive.

- A *third party* is a *privacy stakeholder* other than the PII *principal*, the PII *controller* and the PII *processor*, and the natural persons who are authorized to *process* the *data* under the direct *authority* of the PII *controller* or the PII *processor*.

26. Terms with respect to *Social Responsibility*

Source: [43]

...

- *Accountability* is the state of being answerable for decisions and activities to the *organization*'s *governing bodies*, legal authorities and, more broadly, its *stakeholders*.
- A *consumer* is an individual member of the general public purchasing or using property, *products* or *services* for private purposes.
- A *customer* is an *organization* or individual member of the general public purchasing property, *products* or *services* for commercial, private or public purposes.
- *Due diligence* is a comprehensive, proactive *process* to identify the actual and potential negative social, environmental and economic *impacts* of an *organization*'s decisions and activities over the entire *life cycle* of a *project* or organizational *activity*, with the aim of avoiding and mitigating negative *impacts*.
- An *employee* is an individual in a relationship recognized as an "employment relationship" in national law or practice.
- The *environment* is the natural surroundings in which an *organization* operates, including air, water, land, natural resources, flora, fauna, people, outer space and their interrelationships.
- *Ethical behaviour* is behaviour that is in accordance with accepted principles of right or good conduct in the context of a particular situation and is consistent with *international norms of behaviour*.
- An *impact of an organization* is an *impact* is the positive or negative change to society, economy or the *environment*, wholly or partially resulting from an *organization*'s past and present decisions and *activities*.
- An *initiative for social responsibility* is an initiative is a *programme* or *activity* expressly devoted to meeting a particular aim related to *social responsibility*. Initiatives for social responsibility can be developed, sponsored or administered by any type of organization.
- The *international norms of behaviour* are the expectations of socially responsible organizational behaviour derived from customary international law, generally accepted principles of international law, or intergovernmental agreements that are universally or nearly universally recognized. Although customary international law, generally accepted principles of international law and intergovernmental agreements are directed primarily at states, they express goals and principles to which all organizations can aspire.
- An *organization* is an *entity* or group of people and *facilities* with an arrangement of responsibilities, authorities and relationships and identifiable *objectives*.
- *Organizational governance* is a *system* by which an *organization* makes and implements decisions in pursuit of its *objectives*.
- A *principle* is a fundamental basis for decision making or behaviour.
- A *product* is an article or substance that is offered for sale or is part of a *service* delivered by an *organization*.
- A *service* is an action of an *organization* to meet a demand or need.
- A *social dialogue* is negotiation, consultation or simply exchange of *information* between or among representatives of governments, employers and workers, on matters of common interest relating to economic and social policy.
- *Social responsibility* is the responsibility of an *organization* for the *impacts* of its decisions and activities on society and the *environment*, through *transparent* and *ethical behaviour* that contributes to *sustainable development*, including health and the welfare of society; takes into account the expectations of *stakeholders*; is in *compliance* with applicable law and consistent with *international norms of behaviour*; and is integrated throughout the *organization* and practised in its relationships. Activities include products, services and processes. Relationships refer to an *organization*'s activities within its *sphere of influence*.
- The *sphere of influence* is the range/extent of political, contractual, economic or other relationships through which an *organization* has the *ability* to affect the decisions or *activities* of individuals or *organizations*. Please note that the ability to influence does not, in itself, imply a responsibility to exercise influence.
- A *stakeholder* is an individual or group that has an interest in any decision or activity of an *organization*.
- *Stakeholder engagement* is an *activity* undertaken to create opportunities for dialogue between an *organization* and one or more of its *stakeholders*, with the aim of providing an informed basis for the *organization*'s decisions.

[43] I SO 26000:2010 *Guidance on social responsibility*

- A *supply chain* is a sequence of *activities* or *parties* that provides *products* or *services* to the *organization*.
- *Sustainable development*[44] is development that meets the needs of the present without compromising the ability of future generations to meet their own needs.
- *Transparency* is the openness about decisions and *activities* that affect society, the economy and the *environment*, and willingness to communicate these in a clear, accurate, timely, honest and complete manner.
- A *value chain* is an entire sequence of *activities* or *parties* that provide or receive value in the form of *products* or *services*.
- A *vulnerable group* is a group of 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.
- A *worker* is a person who performs work, whether an *employee* or someone who is self-employed.

[44] Sustainable development is about integrating the goals of a high quality of life, health and prosperity with social justice and maintaining the earth's capacity to support life in all its diversity. These social, economic and environmental goals are interdependent and mutually reinforcing. Sustainable development can be treated as a way of expressing the broader expectations of society as a whole.

27. Terms with respect to *Education*

Source: [45]

…

- An *ability* is a *capacity* to perform an *activity*.
- A *competence* is an *ability* to apply *knowledge* and *skills* to achieve intended results.
- *Knowledge* is facts, *information*, truths, *principles* or understanding acquired through experience or education.
- A *skill* is the *ability* to perform a *task* or *activity* with a specific intended *outcome* acquired through education, *training*, experience or other means.

Source: [46]

- An *organization* is a *person* or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives*.
- An *interested party* (*stakeholder*) is a *person* or *organization* that can affect, be affected by, or perceive itself to be affected by a decision or *activity*.
- A *requirement* is a need or expectation that is stated, generally implied or obligatory. "Generally implied" means that it is custom or common practice for the *organization* and *interested parties* that the need or expectation under consideration is implied.
- A *specified requirement* is one that is stated, for example in *documented information*.
- A *management system* is a set of interrelated or interacting elements of an *organization* to establish *policies* and *objectives* and *processes* to achieve those *objectives*. The system elements include the organization's structure, roles and responsibilities, planning and operation. The scope of a management system may 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.
- The *top management* is the *person* or group of people who directs and controls an *organization* at the highest level. Top management has the power to delegate authority and provide resources within the organization. If the scope of the *management system* covers only part of an organization, then *top management* refers to those who direct and control that part of the *organization*.
- *Policy* is the intentions and direction of an *organization*, as formally expressed by its *top management*.
- An *objective* is a result to be achieved. An objective can be strategic, tactical, or operational.
- An *audit* is a systematic, independent and documented *process* for obtaining *audit evidence* and evaluating it objectively to determine the extent to which the *audit criteria* are fulfilled.
- A *corrective action* is an action to eliminate the cause of a *nonconformity* and to prevent recurrence.
- A *continual improvement* is a recurring activity to enhance *performance*.
- An *educational organization* is an *organization* whose core business is the provision of *educational products* and *educational services*.
- An *educational service* is a *process* that supports acquisition and development of *learners*' *competence* through *teaching*, learning or research.
- An *educational product* (*learning resource*) is tangible or intangible goods used in pedagogical support of an *educational service*. Educational products can be produced by any parties, including learners (3.25).
- A *learner* is a *beneficiary* acquiring and developing *competence* using an *educational service*.
- A *beneficiary* is a *person* or group of people benefiting from the products and services of an *educational organization* and whom the educational organization is obliged to serve by virtue of its *mission*.
- An *educator* is a *person* who performs *teaching* activities. In different contexts, an educator is sometimes referred to as a teacher, a trainer, a coach, a facilitator, a tutor, a consultant, an instructor, a lecturer or a mentor.
- A *curriculum* is *documented information* of what, why, how and how well *learners* should learn in a systematic and intentional way. A curriculum can include, but is not limited to, the learning aims or *objectives*, content, learning outcomes, *teaching* and

[45] ISO/IEC TS 17027:2014 *Conformity assessment — Vocabulary related to competence of persons used for certification of persons*
[46] ISO 21001:2018 *Educational organizations — Management systems for educational organizations — Requirements with guidance for use*

learning methods, *performance* indicators, assessment methods or research plan that are related to learning. It can also be referred to as a *competence* profile, competence referential, *study programme* or teaching plan.

- *Social responsibility* is the responsibility of an *organization* for the impacts of its decisions and activities on society and the environment, through transparent and ethical behaviour that contributes to sustainable development, including health and the welfare of society; takes into account the expectations of *interested parties*; is in compliance with applicable law and consistent with international norms of behaviour; and is integrated throughout the organization and practised in its relationships.

- *Vision* is the aspirations of an *organization* in relation to its desired future condition and duly aligned with its *mission*.

- *Mission* is the reason for being, mandate and scope of an *organization*, translated into the context in which it operates.

- *Strategy* is a *plan* to accomplish the *organization*'s *mission* and achieve the *organization*'s *vision*.

- A *course* is a distinct set of *teaching* and learning activities, designed to meet defined *learning objectives* or *learning outcomes*.

- A *programme* is a consistent set of *courses* designed to meet defined *learning objectives* or learning outcomes and leading to recognition.

- A *person* (individual, human being) is a natural person, who acts as a distinct indivisible entity or is considered as such.

- *Staff* is the set of *persons* who work for and within an *organization*.

- *Usability* is the extent to which a product, service, environment or facility can be used by specified users to achieve specified goals with *effectiveness*, *efficiency* and satisfaction in a specified context of use

- *Accessibility* is the *usability* of a product, service, environment, or facility by people within the widest range of capabilities.

- *Teaching* is the working with *learners* to assist and support them with learning. Working with learners implies designing, leading and following up learning activities. Teaching can combine different roles: content delivery, facilitation, mentorship, community builder and, to a certain extent, counsellor and academic guidance provider.

- *Lifelong learning* is the provision or use of learning opportunities throughout people's lives in order to foster their continuous development.

- *Skill* is a set of know-how that allows a *person* to master an activity and succeed in accomplishing a *task*. Skill can be cognitive, emotional, social or psychomotor.

- *Knowledge* is the facts, *information*, *principles* or understanding acquired through experience, research or education.

- An *ability* is a *capacity* to perform an *activity*.

- A *competence* is an *ability* to apply *knowledge* and *skills* to achieve intended results.