FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/FDIS
81001-1**

ISO/TC **215**

Secretariat: ANSI

Voting begins on:
2020-12-15

Voting terminates on:
2021-02-09

Health software and health IT systems safety, effectiveness and security —

Part 1:
Principles and concepts

Sécurité, efficacité et sûreté des logiciels de santé et des systèmes TI de santé —

Partie 1: Principes et concepts

This draft is submitted to a parallel vote in ISO and in IEC.

Reference number
ISO/FDIS 81001-1:2020(E)

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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

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

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

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

This document was prepared jointly by Technical Committee ISO/TC 215, *Health informatics*, and Technical Committee IEC/TC 62, *Electrical equipment in medical practice*, Subcommittee SC 62A, *Common aspects of electrical equipment used in medical practice*.

A list of all parts in the ISO 81001 and IEC 81001 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

While the benefits of digital health are widely accepted, the potential for inadvertent and adverse impacts on *safety*, *effectiveness* and *security* caused by *health software* and *health IT systems* is also becoming more apparent. Today's sophisticated *health software* and *health IT systems* provide advanced levels of decision support and integrate patient data between *systems*, across organizational lines, and across the continuum of care. In addition to the patient and healthcare *system* benefits this creates, there is also increased likelihood of software-induced adverse *events* causing harm to both patients and healthcare organizations. Design flaws, coding errors, incorrect *implementation* or configuration, data integrity issues, faults in decision support tools, poor alignment with clinical workflows and improper maintenance and use of such *systems* are examples of *events* with the potential to cause *harm*.

Managing *safety*, *effectiveness* and *security* for *health software* and *health IT systems* (including *medical devices*), requires a comprehensive and coordinated approach to optimizing these three properties. Many *organizations* and *roles* are involved throughout the *life cycle* of *health software* and *health IT systems* (see Figure 1). Therefore, a common understanding of the concepts, principles and terminology is important in standardizing the *processes* and inter-organizational communications to support a coordinated approach to managing *safety*, *effectiveness* and *security*. This document takes into account the evolving complex internal and external context in healthcare, including people, technology (hardware/software), *organizations*, *processes*, and external environment.

Annex A provides further information on the rationale for this document, the terms and definitions being used and their relationship to other standards addressing various aspects of *health software* and *health IT systems safety*, *effectiveness* and *security*.

In addition to a common set of terms, definitions and concepts, this document describes eight foundational elements in Clause 5, which support the overarching themes articulated in Clause 4. For each foundational element, there is a "statement" describing each element; a "rationale" explaining why it is important; "key concepts and principles" pertinent for managing *safety*, *effectiveness* and *security*; and high-level guidance on the "approach" *organizations* can take to apply the concepts and principles.

Given the importance of communication between the various *organizations*, *roles* and responsibilities involved across the *life cycle* of *health software* and *health IT systems* for the four foundational cross-organizational elements, additional sub-clauses on communication and information sharing at major transition points are also included for 5.3.2, 5.3.3, 5.3.4 and 5.3.5.

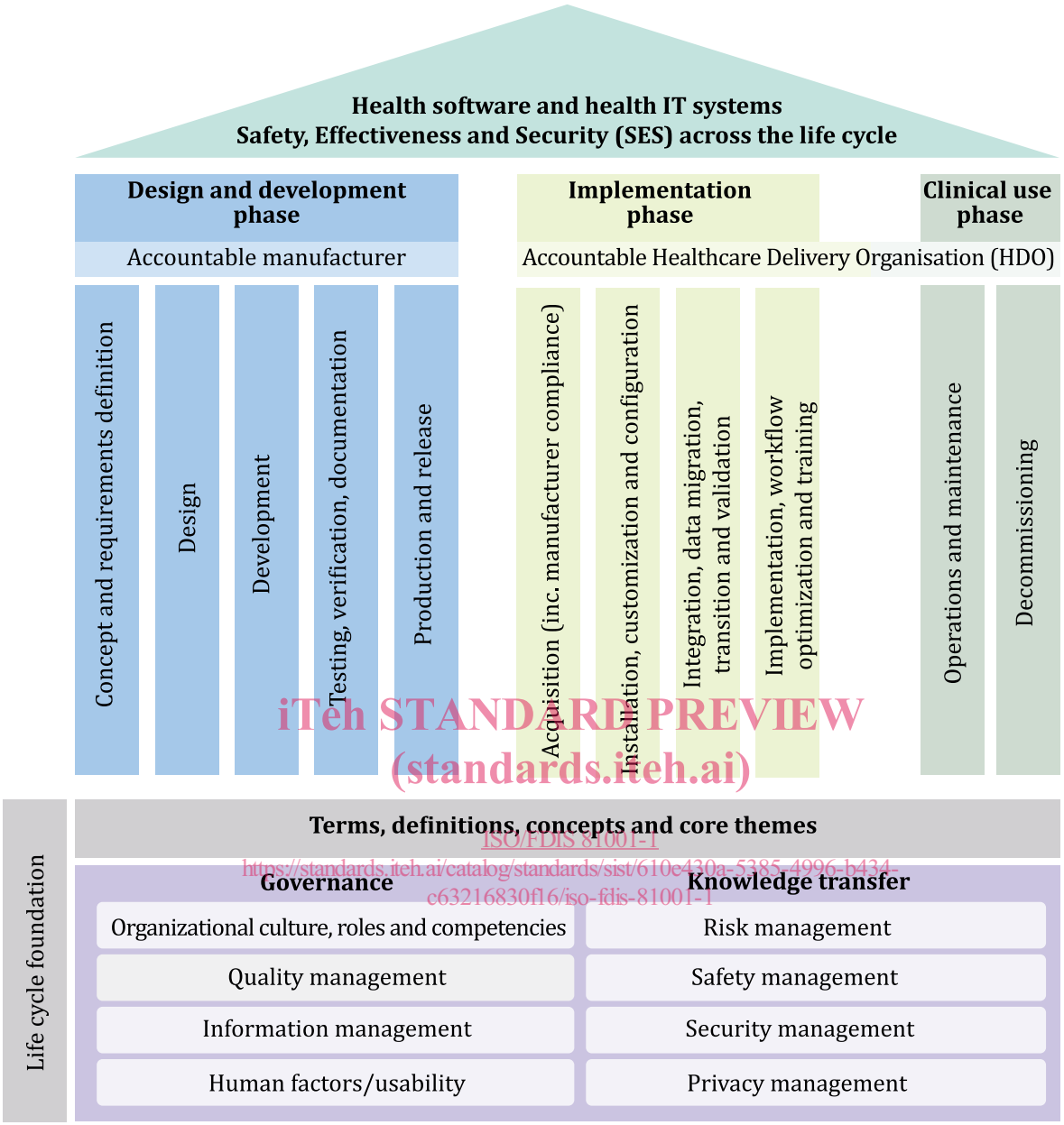

Figure 1 — *Life cycle* framework addressing *safety, effectiveness* and *security* of *health software* and *health IT systems*

Health software and health IT systems safety, effectiveness and security —

Part 1:
Principles and concepts

1 Scope

This document provides the principles, concepts, terms and definitions for *health software* and *health IT systems, key properties* of *safety*, *effectiveness* and *security,* across the full *life cycle*, from concept to decommissioning, as represented in Figure 1. It also identifies the transition points in the *life cycle* where transfers of responsibility occur, and the types of multi-lateral communication that are necessary at these transition points. This document also establishes a coherent concepts and terminology for other standards that address specific aspects of the safety, effectiveness, and security (including privacy) of health software and health IT systems.

This document is applicable to all parties involved in the *health software* and *health IT systems life cycle* including the following:

a) *Organizations*, health informatics professionals and clinical leaders designing, developing, integrating, implementing and operating these *systems* – for example *health software developers* and *medical device manufacturers*, *system integrators*, *system administrators* (including cloud and other IT service providers);

b) Healthcare service delivery *organizations*, healthcare providers and others who use these *systems* in providing health services;

c) Governments, health system funders, monitoring agencies, professional *organizations* and *customers* seeking confidence in *an organization's ability to consistently provide safe, effective and secure health software*, *health IT systems* and services;

d) *Organizations* and interested parties seeking to improve communication in managing *safety*, *effectiveness* and *security risks* through a common understanding of the concepts and terminology used in *safety*, *effectiveness* and *security* management;

e) Providers of training, assessment or advice in *safety*, *effectiveness* and *security risk management* for *health software* and *systems*;

f) *Developers* of related *safety*, *effectiveness* and *security* standards.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

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

NOTE Annex B contains a diagrammatic representation of how the terms used in this document relate conceptually.

3.1 Organizations, people, and roles

3.1.1
administrator
person with *role* (3.1.10) responsible for the ongoing operation of the implemented *health IT system* (3.3.8) and ensuring it is safeguarded and maintained on an ongoing basis

3.1.2
customer
person or *organization* (3.1.8) that could or does receive a *product* (3.3.15) or a service that is intended for or required by this person or *organization*

Note 1 to entry: A *customer* can be internal or external to the *organization*.

[SOURCE: ISO 9000:2015, 3.2.4, modified — Example deleted.]

3.1.3
developer
entity responsible for executing the design and development phase (from concept to release and maintenance) of a *health software* (3.3.9) or *health IT system* (3.3.8)

Note 1 to entry: A *developer* could, for example, be part of a manufacturing *organization* (3.1.8), a supplier of services, or an *healthcare delivery organization* (3.1.4).

3.1.4
healthcare delivery organization
HDO
facility or enterprise such as a clinic or hospital that provides healthcare services

3.1.5
implementer
entity responsible for the clinical installation, workflow optimization, and training of *health software* (3.3.9) and *health IT systems* (3.3.8) in the clinical setting

Note 1 to entry: An *implementer* can be the *manufacturer* (3.1.7), the *healthcare delivery organization* (3.1.4), or a third party.

3.1.6
integrator
entity responsible for the incorporation of *components* (3.3.5) into the *health IT infrastructure* (3.3.7) used by the *healthcare delivery organization* (3.1.4), including technical installation, configuration, and data migration

3.1.7
manufacturer
organization (3.1.8) with responsibility for design or manufacture of a *product* (3.3.15)

3.1.8
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

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

[SOURCE: ISO 9000:2015, 3.2.1, modified — Removed note 2 to entry.]

3.1.9
responsibility agreement
document that fully defines the responsibilities of all relevant stakeholders

Note 1 to entry: This agreement can be a legal document, for example, a contract.

3.1.10
role
function or position

[SOURCE: ISO/HL7 21731:2006]

3.1.11
subject of care
person who seeks to receive, is receiving, or has received healthcare

[SOURCE: ISO 13940:2015, 5.2.1, modified - the words "healthcare actor with a person role" was replaced with "person"]

3.1.12
system owner
senior executive accountable for ensuring the *health IT system* (3.3.8) being acquired and implemented will meet their *organization's* (3.1.8) healthcare delivery services needs for its *intended use* (3.2.7)

3.1.13
top management
executive management
group of people who direct and control an *organization* (3.1.8) and have overall accountability in an *organization*

3.1.14
user
person using the *system* (3.3.17) for a health-related purpose

Note 1 to entry: The user can be the subject of care directly, or an individual assisting (as proxy for) the subject of care.

3.2 Key properties and processes

3.2.1
change management
process (3.2.10) for recording, coordination, approval and monitoring of all changes

[SOURCE: ISO/IEC TS 22237-7:2018, 3.1.3]

3.2.2
change-release management
process (3.2.10) that ensures that all changes to the *health IT infrastructure* (and its *components* (3.3.5) are assessed, approved, implemented and reviewed in a controlled manner and that changes are delivered, distributed, and tracked, leading to release of the change in a controlled manner with appropriate input and output with *configuration management* (3.2.4)

3.2.3
clinical change management
strategic and systematic *process* (3.2.10) that supports people and their *organizations* (3.1.8) in the successful transition and adoption of electronic health solutions, with a focus on outcomes including solution adoption by *users* (3.1.14) and the realization of benefits

Note 1 to entry: Adapted from Reference [39].

3.2.4
configuration management
process (3.2.10) that ensures that configuration information of *components* (3.3.5) within the *health IT infrastructure* (3.3.7) are defined and maintained in an accurate and controlled manner, and provides a mechanism for identifying, controlling and tracking versions of the *health IT infrastructure*

Note 1 to entry: Adapted from ISO/IEC 20000-1:2018, 8.2.6.

3.2.5
effectiveness
ability to produce the intended result

3.2.6
implementation
life cycle (3.3.12) phase at the end of which the hardware, software and procedures of the *system* (3.3.17) considered become operational

[SOURCE: ISO/IEC 2382:2015, 2122692, modified — Changed "system development" to "*life cycle*" and delete notes to entry.]

3.2.7
intended use
intended purpose
use for which a *product* (3.3.15), *process* (3.2.10) or service is intended according to the specifications, instructions and information provided by the *manufacturer* (3.1.7)

Note 1 to entry: The intended medical indication, patient population, part of the body or type of tissue interacted with, *user* profile, use environment, and operating principle are typical elements of the *intended use*.

[SOURCE: ISO/IEC Guide 63:2019, 3.4, modified — Added admitted term *intended purpose*.]

3.2.8
key properties
three *risk management* (3.4.16) characteristics of *safety* (3.2.12), *effectiveness* (3.2.5), and *security* (3.2.13)

3.2.9
privacy
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

[SOURCE: ISO/TS 27790:2009, 3.56]

3.2.10
process
set of interrelated or interacting activities that use inputs to deliver an intended result

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

3.2.11
quality
degree to which all the properties and characteristics of a *product* (3.3.15), *process* (3.2.10), or service satisfy the requirements which ensue from the purpose for which that *product*, *process*, or service is used

[SOURCE: ISO/TS 13972:2015, 2.45, modified — Deleted "to be".]

3.2.12
safety
freedom from unacceptable *risk* (3.4.10)

[SOURCE: ISO/IEC Guide 63:2019, 3.16]

3.2.13
security
cybersecurity
state where information and *systems* (3.3.17) are protected from unauthorized activities, such as access, use, disclosure, disruption, modification, or destruction to a degree that the *risks* (3.4.10) related to violation of confidentiality, integrity, and availability are maintained at an acceptable level throughout the *life cycle* (3.3.12)

3.2.14
security capability
broad category of technical, administrative or organizational controls to manage *risks* (3.4.10) to confidentiality, integrity, availability and accountability of data and *systems* (3.3.17)

3.2.15
usability
characteristic of the *user* (3.1.14) interface that facilitates use and thereby establishes *effectiveness* (3.2.5), efficiency and *user* satisfaction in the *intended use* (3.2.7) environment

Note 1 to entry: All aspects of *usability*, including *effectiveness*, efficiency and *user* satisfaction, can either increase or decrease *safety* (3.2.12).

[SOURCE: IEC 62366-1:2015, 3.16]

3.2.16
verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

Note 1 to entry: 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.

Note 2 to entry: The activities carried out for *verification* are sometimes called a qualification *process* (3.2.10).

Note 3 to entry: The word "verified" is used to designate the corresponding status.

[SOURCE: ISO 9000:2015, 3.8.12]

3.3 Health information and technology

3.3.1
accompanying information
accompanying document
accompanying documentation
information accompanying or marked on a *health IT* (3.3.6), *product* (3.3.15) or accessory for the *user* (3.1.14) or those accountable for the installation, use, processing, maintenance, decommissioning and disposal of the *medical device* (3.3.13) or accessory, particularly regarding safe use

3.3.2
asset
physical or digital entity that has value to an individual, an *organization* (3.1.8) or a government

[SOURCE: ISO/IEC 27032:2012, 4.6, modified — "anything" has been replaced by "physical entity or digital entity".]

3.3.3
cloud computing
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

[SOURCE: ISO/IEC 17788:2014, 3.25]

3.3.4
cloud service
one or more capabilities offered via *cloud computing* (3.3.3) invoked using a defined interface

[SOURCE: ISO/IEC 17788:2014, 3.2.8]

3.3.5
component
collection of *system* (3.3.17) resources that (a) forms a physical or logical part of the *system*, (b) has specified functions and interfaces, and (c) is treated (e.g., by policies or specifications) as existing independently of other parts of the *system*

[SOURCE: IETF RFC 4949, modified — Note 1 deleted.]

3.3.6
health information technology
health IT
documented and intended application of information technology for the collection, storage, processing, retrieval, and communication of information relevant to health, patient care, and well-being

3.3.7
health IT infrastructure
combined set of IT *assets* (3.3.2) available to the individual or *organization* (3.1.8) for developing, configuring, integrating, maintaining, and using IT services and supporting health, patient care and other organizational objectives

Note 1 to entry: Health IT infrastructure can include the following:

a) data and information;

b) *health software* (3.3.9);

c) *medical devices* (3.3.13);

d) IT hardware and services including mobile and desktop devices, *IT networks* (3.3.11), data centres, *security* (3.2.13), software development, IT operations and externally provided services such as internet, software-as-a-service and *cloud computing* (3.3.3);

e) people, and their qualifications, skills and experience;

f) technical procedures and documentation to manage and support the *health IT infrastructure*;

g) health IT *systems* (3.3.8) that are configured and implemented to address organizational objectives by leveraging the above *assets* (3.3.2);

h) intangibles, such as reputation and image.

3.3.8
health IT system
combination of interacting *health IT* (3.3.6) elements that is configured and implemented to support and enable an individual or *organization's* (3.1.8) specific health objectives

Note 1 to entry: Such elements include *health software* (3.3.9), *medical devices* (3.3.13), IT hardware, interfaces, data, procedures and documentation).

3.3.9
health software
software intended to be used specifically for managing, maintaining, or improving health of individual persons, or the delivery of care, or which has been developed for the purpose of being incorporated into a *medical device* (3.3.13)

Note 1 to entry: *Health software* fully includes what is considered software as a *medical device*.

3.3.10
interoperability
ability of two or more *systems* (3.3.17) or *components* (3.3.5) to exchange information and to use the information that has been exchanged

[SOURCE: Reference[50]]

3.3.11
IT network
system (3.3.17) or *systems* composed of communicating nodes and transmission links to provide physically linked or wireless transmission between two or more specified communication nodes

Note 1 to entry: Adapted from IEC 61907:2009, 3.1.1.

3.3.12
life cycle
series of all phases in the life of a *product* (3.3.15) or *system* (3.3.17), from the initial conception to final decommissioning and disposal

[SOURCE: ISO/IEC Guide 63:2019, 3.5, modified — "medical device" has been replaced with "*product* or *system*".]

3.3.13
medical device
instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article, intended by the *manufacturer* (3.1.7) to be used, alone or in combination, for human beings, for one or more of the specific medical purpose(s) of

— diagnosis, prevention, monitoring, treatment or alleviation of disease,

— diagnosis, monitoring, treatment, alleviation of or compensation for an injury,

— investigation, replacement, modification, or support of the anatomy or of a physiological *process*,

— supporting or sustaining life,

— control of conception,

— disinfection of *medical devices*,

— providing information by means of in vitro examination of specimens derived from the human body,

and which does not achieve its primary intended action by pharmacological, immunological or metabolic means, in or on the human body, but which can be assisted in its intended function by such means

Note 1 to entry: *Products* (3.3.15) which can be considered to be *medical devices* in some jurisdictions but not in others include:

— disinfection substances,

— aids for persons with disabilities,

— devices incorporating animal and/or human tissues,

— devices for in-vitro fertilization or assisted reproductive technologies.

[SOURCE: ISO/IEC Guide 63:2019, 3.7]

3.3.14
personal health information
information about an identifiable person that relates to the physical or mental health of the individual

Note 1 to entry: To provision of health services to the individual and that may include:

a) information about the registration of the individual for the provision of health services;

b) information about payments or eligibility for health care in respect to the individual;

c) a number, symbol, or particular assigned to an individual to uniquely identify the individual for health purposes;

d) any information about the individual that is collected in the course of the provision of health services to the individual;

e) information derived from the testing or examination of a body part or bodily substance;

f) identification of a person (e.g. a health professional) as provider of healthcare to the individual.

Note 2 to entry: *Personal health information* does not include information that, either by itself or when combined with other information available to the holder, is anonymized, the identity of the individual who is the subject of the information cannot be ascertained from the information.

[SOURCE: ISO 27799:2016, 3.8]

3.3.15
product
output of an *organization* (3.1.8) that can be produced without any transaction taking place between the *organization* and the *customer* (3.1.2)

Note 1 to entry: Production of a *product* is achieved without any transaction necessarily taking place between provider and *customer*, but can often involve this service element upon its delivery to the *customer*.

Note 2 to entry: The dominant element of a *product* is that it is generally tangible.

[SOURCE: ISO 9001:2015, 3.7.6, modified — Note 3 to entry deleted.]

3.3.16
sociotechnical ecosystem

complex ‘ecosystem’ or ‘sociotechnical system’ environment where the software is tightly integrated with other *systems* (3.3.17), technologies, infrastructure, and domains (people, *organizations* (3.1.8) and external environments) and where it is configured to support local clinical and business *processes* (3.2.10)

3.3.17
system
combination of interacting elements organized to achieve one or more stated purposes

[SOURCE: ISO/IEC/IEEE 15288: 2015, 4.1.46, modified — Notes to entry deleted.]

3.4 Risk management

3.4.1
assurance case
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)

Note 1 to entry: 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.

[SOURCE: ISO/IEC/IEEE 15026-1:2019, 3.1.2]

3.4.2
event
occurrence or change of a particular set of circumstances

Note 1 to entry: An *event* can be one or more occurrences and can have several causes.

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

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

[SOURCE: ISO Guide 73:2009, 3.5.1.3, modified — Note 4 to entry deleted.]

3.4.3
exploit
defined way to breach the *security* (3.2.13) of *systems* (3.3.17) through *vulnerability* (3.4.22)

[SOURCE: ISO/IEC 27039:2015, 2.9, modified — "information" removed.]

3.4.4
exposure
extent to which an *organization* (3.1.8) and/or stakeholder is subject to an *event* (3.4.2)

[SOURCE: ISO Guide 73:2009, 3.6.1.2]

3.4.5
harm
injury or damage to the health of people, or damage to property or the environment

[SOURCE: ISO/IEC Guide 63:2019, 3.1]

3.4.6
hazard
potential source of *harm* (3.4.5)

[SOURCE: ISO/IEC Guide 63:2019, 3.2]

3.4.7
hazardous situation
circumstance in which people, property or the environment is/are exposed to one or more *hazards* (3.4.6)

[SOURCE: ISO/IEC Guide 63:2019, 3.3]

3.4.8
reasonably foreseeable misuse
use of a *product* (3.3.15) or *system* (3.3.17) in a way not intended but which can result from readily predictable human behaviour

Note 1 to entry: Readily predictable human behaviour includes the behaviour of all types of *users* (3.1.14), e.g., lay and professional *users*.

Note 2 to entry: *Reasonably foreseeable misuse* can be intentional or unintentional.

[SOURCE: ISO/IEC Guide 63:2019, 3.8, modified — "by the manufacturer" Removed.]

3.4.9
residual risk
risk (3.4.10) remaining after *risk control* (3.4.13) measures have been implemented

[SOURCE: ISO/IEC Guide 63:2019, 3.9]