DRAFT INTERNATIONAL STANDARD
IEC/DIS 81001-5-1

ISO/TC **215** Secretariat: **ANSI**

Voting begins on:
2020-12-09

Voting terminates on:
2021-03-03

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

Part 5-1:
Security — Activities in the product life cycle

ICS: 35.240.80; 35.080

iTeh STANDARD PREVIEW
(standards.iteh.ai)

IEC/DIS 81001-5-1
https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21-05f80dda507a/iec-dis-81001-5-1

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

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

Reference number
IEC/DIS 81001-5-1:2020(E)

© IEC 2020

iTeh STANDARD PREVIEW
(standards.iteh.ai)

IEC/DIS 81001-5-1
https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21-05f80dda507a/iec-dis-81001-5-1

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/DIS 81001-5-1
https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21-05f80dda507a/iec-dis-81001-5-1

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/DIS 81001-5-1
https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21-05f80dda507a/iec-dis-81001-5-1

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

Health software and health IT systems safety, effectiveness and security
Part 5: Security
Part 5-1: Security - Activities in the product life cycle

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/DIS 81001-5-1
https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21-05f80dda507a/iec-dis-81001-5-1

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

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

This Committee Draft of future International Standard IEC 81001-5-1 has been prepared by subcommittee 62A/ JWG7 of IEC technical committee 62 and ISO/TC 215/JWG 7.

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.
This document has been drafted in accordance with the ISO/IEC Directives, Part 2.
The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

> The National Committees are requested to note that for this document the stability date is 2026
> THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE DELETED AT THE PUBLICATION STAGE.

Introduction

This International Standard specifies supplementary ACTIVITIES that will be performed by the MANUFACTURER of HEALTH SOFTWARE – including software incorporated in medical devices –as a part of a secure development LIFE CYCLE. This document can therefore support conformity to IEC 62443-4-1.

This document is intended to supply minimum best practices for a secure software LIFE CYCLE. Local legislation and regulation have to be considered.

PROCESS requirements have been derived from IEC 62443-4-1 PRODUCT LIFE CYCLE Management. Implementations of these specifications will extend existing PROCESSES at the MANUFACTURER's organization –notably existing PROCESSES conforming to IEC 62304.

This document specifies ACTIVITIES for HEALTH SOFTWARE, the LIFE CYCLE of which can be part of an incorporating PRODUCT project. Some ACTIVITIES specified in this document depend on input and support from the PRODUCT LIFE CYCLE (for example to define specific criteria). Examples include:

- RISK MANAGEMENT
- Requirements
- Testing
- Post-Market

In cases where ACTIVITIES for HEALTH SOFTWARE need support from PROCESSES at the PRODUCT level, this document specifies respective requirements beyond the HEALTH SOFTWARE LIFE CYCLE.

Similar to IEC 62304, this document does not prescribe a specific system of PROCESSES, but it requires that certain ACTIVITIES are being performed during the HEALTH SOFTWARE LIFE CYCLE.

This document specifies ACTIVITIES to be performed by the MANUFACTURER. For the purpose of this document this includes all entities responsible for construction ACTIVITIES in the LIFE CYCLE of HEALTH SOFTWARE.

Clause four specifies that MANUFACTURERS develop and maintain HEALTH SOFTWARE within a quality management system (see 4.1) and a RISK MANAGEMENT SYSTEM (4.2).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/DIS 81001-5-1
https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e5-ad21-05f80dda507a/iec-dis-81001-5-1

Clauses five to eight specify ACTIVITIES and resulting output as part of the software LIFE CYCLE PROCESS implemented by the MANUFACTURER. These specifications are arranged in the ordering of IEC 62304.

Clauses nine and ten specify ACTIVITIES and resulting output as part of the problem resolution PROCESS and quality management system respectively, implemented by the MANUFACTURER.

The scope of this document is limited to HEALTH SOFTWARE and its connectivity to its INTENDED ENVIRONMENT OF USE, based on IEC 62304, but with emphasis on information SECURITY.

For expression of provisions in this document,

— "can" is used to describe a possibility or capability; and

— "must" is used to express an external constraint.

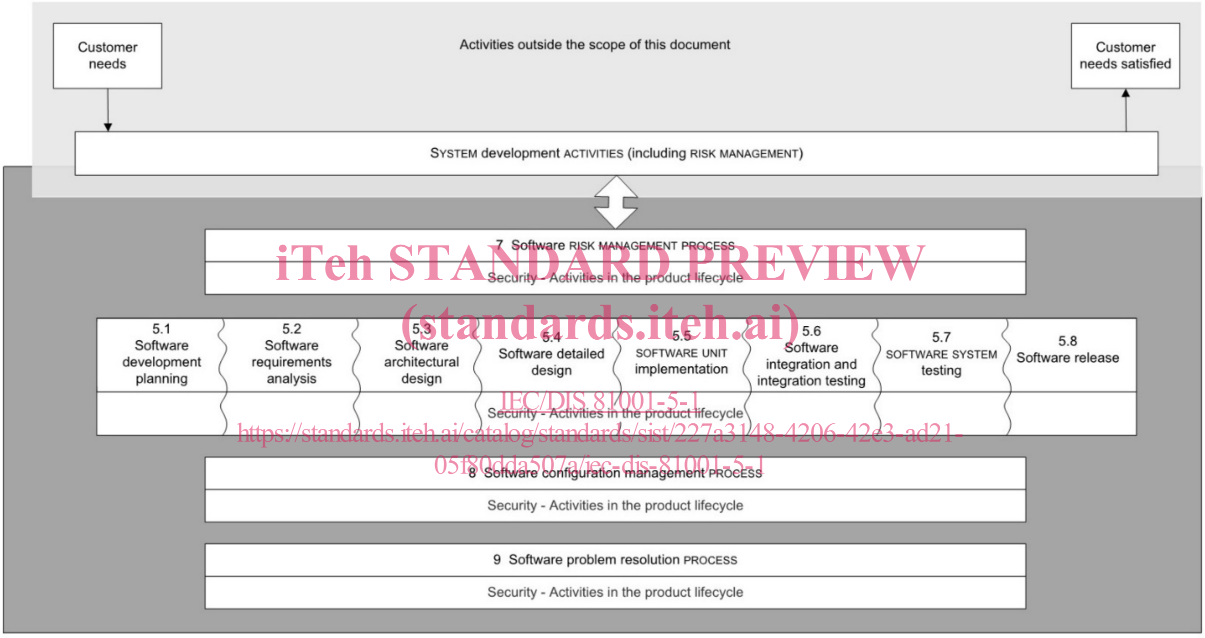
Note: HEALTH SOFTWARE can be placed on the market as software, incorporated into medical devices, as software that in itself is considered a medical device, or incorporated into a general-purpose computing platform.

Health software and health IT systems safety, effectiveness and security
Part 5: Security
Part 5-1: Security - Activities in the product life cycle

1 Scope

1.1 * Purpose

This document defines the LIFE CYCLE requirements for development and maintenance of HEALTH SOFTWARE needed to support conformity to IEC 62443-4-1 – taking the specific needs for HEALTH SOFTWARE into account. The set of PROCESSES, ACTIVITIES, and TASKS described in this document establishes a common framework for secure HEALTH SOFTWARE LIFE CYCLE PROCESSES.


Customer needs
Activities outside the scope of this document
Customer needs satisfied
SYSTEM development ACTIVITIES (including RISK MANAGEMENT)
7 Software RISK MANAGEMENT PROCESS
Security - Activities in the product lifecycle
5.1 Software development planning
5.2 Software requirements analysis
5.3 Software architectural design
5.4 Software detailed design
5.5 SOFTWARE UNIT implementation
5.6 Software integration and integration testing
5.7 SOFTWARE SYSTEM testing
5.8 Software release
Security - Activities in the product lifecycle
8 Software configuration management PROCESS
Security - Activities in the product lifecycle
9 Software problem resolution PROCESS
Security - Activities in the product lifecycle

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/DIS 81001-5-1
https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21-05f80dda507a/iec-dis-81001-5-1

Fig. 1: HEALTH SOFTWARE LIFE CYCLE PROCESSES (derived from IEC 62304, Ed 1.1)

The purpose is to increase the information SECURITY of HEALTH SOFTWARE by establishing certain ACTIVITIES and TASKS in the HEALTH SOFTWARE LIFE CYCLE PROCESSES and also by increasing the SECURITY of SOFTWARE LIFE CYCLE PROCESSES themselves.

It is important to maintain an appropriate balance of the key properties SAFETY, effectiveness and SECURITY as discussed in IEC 81001-1.

This document excludes specification of ACCOMPANYING DOCUMENTATION contents.

1.2 * Field of application

This document applies to the development and maintenance of HEALTH SOFTWARE by a MANUFACTURER, but recognizes the critical importance of bi-lateral communication with organizations (e.g. HDOs) who have SECURITY responsibilities for the HEALTH SOFTWARE and the systems it is incorporated into, once the software has been developed and released. The IEC/ISO 81001-5 series of standards (for which this is part 1, is therefore being designed to include future parts addressing SECURITY that apply to the implementation, operations and use phases of the LIFE CYCLE for organizations such as HDOs.

Medical device software is a subset of HEALTH SOFTWARE. Therefore, this document applies to:

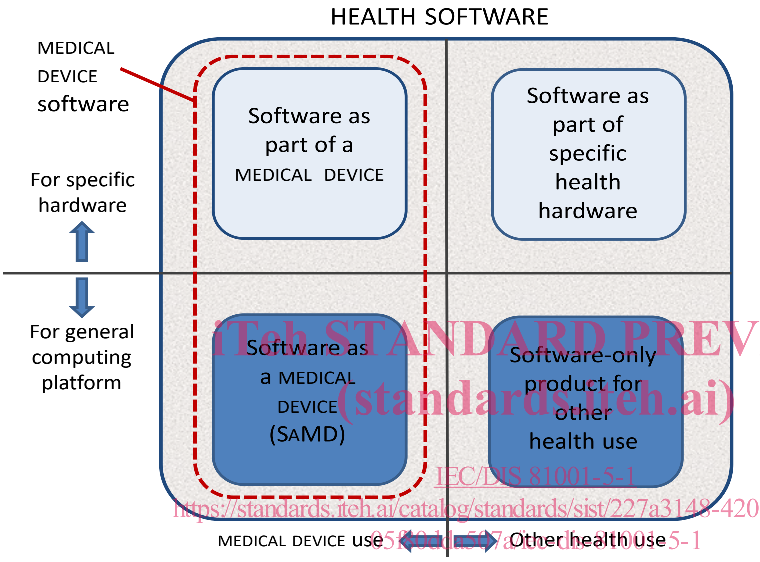
– Software as part of a medical device;

– Software as part of hardware specifically intended for health use;

– Software as a medical device (SaMD); and

– Software-only PRODUCT for other health use.

Note: In this document, the scope of software considered part of the LIFE CYCLE ACTIVITIES for secure HEALTH SOFTWARE is larger and includes more software (drivers, platforms, operating systems) than for SAFETY, because for SECURITY the focus will be on any use including foreseeable unauthorized access rather than just the INTENDED USE.


HEALTH SOFTWARE
MEDICAL DEVICE software
For specific hardware
For general computing platform
Software as part of a MEDICAL DEVICE
Software as part of specific health hardware
Software as a MEDICAL DEVICE (SAMD)
Software-only product for other health use
MEDICAL DEVICE use
Other health use

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/DIS 81001-5-1
https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21-05f40da5f7a3/iec-dis-81001-5-1

Fig. 2: HEALTH SOFTWARE field of application (source: IEC 62304 Ed 2)

1.3 Conformance

HEALTH SOFTWARE conformance with this document is defined as implementing all of the PROCESSES, ACTIVITIES, and TASKS identified in the normative parts of this document - with the exception of Annex F.

Conformance of TRANSITIONAL HEALTH SOFTWARE with Annex F of this document is defined as only implementing the PROCESSES, ACTIVITIES, and TASKS identified in Annex F of this document.

Conformance is determined by inspection and establishing traceability of the PROCESSES, ACTIVITIES and TASKS required.

The quality management system may be implemented according to ISO 13485 or other equivalent quality management system standards.

IEC 62304 specifies ACTIVITIES, based on the software SAFETY classification. The required ACTIVITIES are indicated in the normative text of IEC 62304 as "[Class A, B, C]", "[Class B, C]" or "[Class C]", indicating that they are required selectively depending on the classification of the software to which they apply. The requirements in this document have a special focus on information SECURITY and therefore do not follow the concept of SAFETY classes. For conformity to this document the selection of ACTIVITIES is independent of SAFETY classes.

Implementing the PROCESSES, ACTIVITIES and TASKS specified in this document is sufficient to implement the PROCESS requirements of IEC 62443-4-1. MANUFACTURERS may implement the specifications for Annex E in order to achieve full conformity to IEC 62443-4-1.

This document requires establishing one or more PROCESSES that comprise of identified ACTIVITIES. The LIFE CYCLE PROCESSES shall implement these ACTIVITIES. None of the requirements in this document requires to implement these ACTIVITIES as one single PROCESS or as separate PROCESSES. The ACTIVITIES specified in this document will typically be part of an existing LIFE CYCLE PROCESS.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

- IEC Electropedia: available at www.electropedia.org/
- ISO Online browsing platform: available at www.iso.org/obp

3.1

ACCOMPANYING DOCUMENTATION

documentation accompanying a HEALTH SOFTWARE and HEALTH IT SYSTEM or an accessory, containing information for the responsible organization or operator, particularly regarding SAFETY

[SOURCE: ISO 81001-1:2020, 3.1]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.2

ACTIVITY

set of one or more interrelated or interacting TASKS

IEC/DIS 81001-5-1
https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21-05f80dda507a/iec-dis-81001-5-1

[SOURCE: IEC 62304:2021, 3.1]

3.3

ARCHITECTURE

fundamental concepts or properties of a system in its environment, embodied in its elements, relationships, and in the principles of its design and evolution

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.216, definition1]

3.4

ASSET

physical or digital entity that has value to an individual, an organization or a government

Note 1 to entry: As per the definition for ASSET this can include the following:

a) data and information;

b) HEALTH SOFTWARE and software needed for its operation;

c) hardware components such as computers, mobile devices, servers, databases, and networks;

d) services, including SECURITY, software development, IT operations and externally provided services such as data centres, internet and software-as-a-service and cloud solutions;

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 that are configured and implemented to address organizational objectives by leveraging the ASSETS; AND

h) intangibles, such as reputation and image.

[SOURCE: ISO 81001-1:2020, 3.3]

3.5

ATTACK

attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an ASSET

[SOURCE: ISO/IEC 27000:2018, 2.3]

3.6

ATTACK SURFACE

physical and functional interfaces of a system that can be accessed and, therefore, potentially exploited by an attacker

[SOURCE: ISO/IEC 62443-4-1, 3.1.7]

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/DIS 81001-5-1
https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-43e3-ad21-05f80dda507a/iec-dis-81001-5-1

3.7

AVAILABILITY

property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO/IEC 27000:2018, 2.9]

3.8

CONFIDENTIALITY

property that information is not made available or disclosed to unauthorized individuals, entities, or PROCESSES

[SOURCE: ISO/IEC 24767-1:2008, 2.1.2]

3.9

CONFIGURATION ITEM

entity that can be uniquely identified at a given reference point

[SOURCE: IEC 62304:2021]

3.10

CONFIGURATION MANAGEMENT

PROCESS ensuring consistency of CONFIGURATION ITEMS by using mechanisms for identifying, controlling and tracking versions of CONFIGURATION ITEMS

[SOURCE: IEC 81001-1:2020, modified]

3.11

DEFENSE-IN-DEPTH

approach to defend the system against any particular ATTACK using several independent methods

Note to entry: DEFENSE-IN-DEPTH implies layers of SECURITY and detection, even on single systems, and provides the following features:

- is based on the idea that any one layer of protection, can and probably will be defeated;
- attackers are faced with breaking through or bypassing each layer without being detected;
- a flaw in one layer can be mitigated by capabilities in other layers;
- system SECURITY becomes a set of layers within the overall network SECURITY; and
- each layer should be autonomous and not rely on the same functionality nor have the same failure modes as the other layers.

[SOURCE: IEC 62443-4-1: 3.1.15]

3.12

EXPLOIT (noun)

defined way to breach the SECURITY of information systems through some VULNERABILITY

[SOURCE: ISO/IEC 27039:2015]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.13

HEALTH IT INFRASTRUCTURE

combined set of IT ASSETS available to the individual or organization for developing, configuring, integrating, maintaining, and using IT services and supporting health, patient care and other organizational objectives

IEC/DIS 81001-5-1
https://standards.iteh.ai/catalog/standards/sist/227a6148-4206-42e5-ad21-05180dda507a/iec-dis-81001-5-1

[SOURCE: ISO 81001-1:202x, 3.21]

3.14

HEALTH IT SYSTEM

a combination of interacting health information elements (including HEALTH SOFTWARE, medical devices, IT hardware, interfaces, data, procedures and documentation) that is configured and implemented to support and enable an individual or organization's specific health objectives

[SOURCE: ISO 81001-1:2020, 3.22]

3.15

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

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

[SOURCE: ISO 81001-1:2020, 3.23]

3.16

HEALTHCARE DELIVERY ORGANIZATION

HDO

facility or enterprise such as a clinic or hospital that provides healthcare services

[SOURCE: ISO 81001-1:2020, 3.24]

3.17

INTEGRITY

property of accuracy and completeness

[SOURCE: ISO/IEC 27000:2018, 2.40]

3.18

INTENDED ENVIRONMENT OF USE

conditions and setting in which users interact with the HEALTH SOFTWARE – as specified by the MANUFACTURER

3.19

INTENDED USE

INTENDED PURPOSE

use for which a PRODUCT, PROCESS or service is intended according to the specifications, instructions and information provided by the MANUFACTURER

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/DIS 81001-5-1
https://standards.iteh.ai/catalog/standards/sist/227a5148-4206-42e5-ad21-05f80dda507a/iec-dis-81001-5-1

[SOURCE: ISO 81001-1:2020, 3.28, note 1 to entry modified – "USE ENVIRONMENT" replaced by "INTENDED ENVIRONMENT OF USE".]

3.20

LIFE CYCLE

series of all phases in the life of a PRODUCT or system, from the initial conception to final decommissioning and disposal

[SOURCE: ISO 81001-1:2020, 3.32]

3.21

MAINTAINED SOFTWARE

SOFTWARE ITEM for which the MANUFACTURER will assume the risk related to SECURITY

Note to entry: See also Annex A.3

3.22

MANUFACTURER

natural or legal person responsible for construction ACTIVITIES in the LIFE CYCLE of HEALTH SOFTWARE

Note 1 to entry: Construction includes ACTIVITIES for conception, design, implementation, packaging, distribution, maintenance of HEALTH SOFTWARE.

Note 2 to entry: Responsibility extends to supporting ACTIVITIES during operations.

Note 3 to entry: Responsibility can be with multiple entities along the supply chain, with service providers, or with entities at different stages in the LIFE CYCLE.

Note 4 to entry: Independent of this, any specific legal accountability is defined by contracts and legislation.

3.23

PROCESS

set of interrelated or interacting ACTIVITIES that use inputs to deliver an intended result (outcome)

[SOURCE: ISO 81001-1:202x, 3.38, modified – added “(outcome)” after “result”.]

3.24

PRODUCT

output of an organization that can be produced without any transaction taking place between the organization and the customer

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

[SOURCE: ISO 81001-1:2020, 3.39]

IEC/DIS 81001-5-1
https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21-03f80dda507a/iec-dis-81001-5-1

3.25

REQUIRED SOFTWARE

SOFTWARE ITEM for which the MANUFACTURER will consider SECURITY-related risks known before release of the HEALTH SOFTWARE

Note to entry: this includes SUPPORTED SOFTWARE. See Annex A.3.

3.26

RESIDUAL RISK

risk remaining after RISK CONTROL measures have been implemented

[SOURCE: ISO 81001-1:2020, 3.42]

3.27

RISK CONTROL

PROCESS in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels

[SOURCE: ISO 81001-1:2020, 3.47]

3.28

RISK MANAGEMENT

systematic application of management policies, procedures and practices to the TASKS of analysing, evaluating, controlling and monitoring risk

[SOURCE: ISO 81001-1:2020, 3.50]

3.29

SAFETY

freedom from unacceptable risk

Note 1 to entry: In the context of SAFETY, risk is the combination of probability of occurrence of harm and severity of harm (see ISO/IEC Guide 51:2014).

Note 2 to entry: SECURITY incidents can lead to harm and can therefore have an impact on SAFETY.

[SOURCE: ISO 81001-1:2020, 3.55, modified – added notes to entry.]

3.30

SECURITY

CYBERSECURITY

A state where information and systems are protected from unauthorized ACTIVITIES, such as access, use, disclosure, disruption, modification, or destruction to a degree that the related risks to CONFIDENTIALITY, INTEGRITY, and AVAILABILITY are maintained at an acceptable level throughout the LIFE CYCLE

[SOURCE: ISO 81001-1:2020, 3.56]

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC/DIS 81001-5-1
https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21-05f80dda507a/iec-dis-81001-5-1

3.31

SECURITY CAPABILITY

broad category of technical, administrative or organizational controls to manage risks to CONFIDENTIALITY, INTEGRITY, AVAILABILITY and accountability of data and systems

[SOURCE: ISO 81001-1:2020, 3.57]

3.32

SECURITY CONTEXT

minimum requirements and assumptions about the environment of HEALTH SOFTWARE - derived from the INTENDED ENVIRONMENT OF USE at PRODUCT-level, considering also the configuration and integration of HEALTH SOFTWARE and taking into account foreseeable unauthorized or unintended access

3.33

SOFTWARE COMPOSITION ANALYSIS

(electronic) analysis of binaries.

Note to entry: SOFTWARE COMPOSITION ANALYSIS can be supported by tools or online services.

3.34

SOFTWARE ITEM

identifiable part of a computer program, i.e. source code, object code, control code, control data, or a collection of these items

[SOURCE: IEC 62304:2021, 3.32]

3.35

SOFTWARE MAINTENANCE

modification of HEALTH SOFTWARE after release for INTENDED USE, for one or more of the following reasons:

a) corrective, as fixing faults;

b) adaptive, as adapting to new hardware or software platform;

c) perfective, as implementing new requirements;

d) preventive, as making the PRODUCT more maintainable.

Note 1 to entry: See also ISO/IEC 14764:2006, 3.10.

[SOURCE: IEC 82304-1:2016, 3.21, modified – In the definition, the words "HEALTH SOFTWARE PRODUCT" have been replaced by "HEALTH SOFTWARE", and reference 3.10 has been added to the note to entry; and “hard-“ has been replaced by “hardware”]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.36

SUPPORTED SOFTWARE

SOFTWARE ITEM for which the MANUFACTURER will notify the customer regarding known risks related to SECURITY

IEC/DIS 81001-5-1
https://standards.iteh.ai/catalog/standards/sist/227a3148-4206-42e3-ad21-05f80dda507a/iec-dis-81001-5-1

Note to entry: this includes MAINTAINED SOFTWARE. See Annex A.3

3.37

TASK

single piece of work that needs to be done to achieve a specific goal

[SOURCE: IEC 62304:2021, 3.38, modified: to achieve a specific goal]

3.38

THREAT

potential for violation of SECURITY, which exists when there is a circumstance, capability, action, or event that could breach SECURITY and cause damage to CONFIDENTIALITY, INTEGRITY, AVAILABILITY of information ASSETS

[SOURCE: ISO 81001-1:2020, 3.62]

3.39

THREAT MODEL

documented result of the THREAT MODELLING ACTIVITY