62A/1428/FDIS

FINAL DRAFT INTERNATIONAL STANDARD (FDIS)

PROJECT NUMBER:	
ISO 81001-1 ED1	
DATE OF CIRCULATION:	CLOSING DATE FOR VOTING:
2020-12-18	**2021-01-29**
SUPERSEDES DOCUMENTS:	
62A/1370/CDV, 62A/1385A/RVC	

IEC SC 62A : COMMON ASPECTS OF ELECTRICAL EQUIPMENT USED IN MEDICAL PRACTICE	
SECRETARIAT:	SECRETARY:
United States of America	Ms Hae Choe
OF INTEREST TO THE FOLLOWING COMMITTEES:	HORIZONTAL STANDARD:
SC 22E,SC 62B,SC 62C,SC 62D,TC 65,TC 66,TC 76,TC 77,TC 85,TC 96,TC 106,TC 108,TC 111,CIS/B	☐

FUNCTIONS CONCERNED:

☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☒ SAFETY

☐ SUBMITTED FOR CENELEC PARALLEL VOTING	☒ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

This document is a draft distributed for approval. It 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, Final 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 document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

Health software and health IT systems safety, effectiveness and security — Part 1: Principles and concepts

PROPOSED STABILITY DATE: 2024

NOTE FROM TC/SC OFFICERS:

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)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) 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.

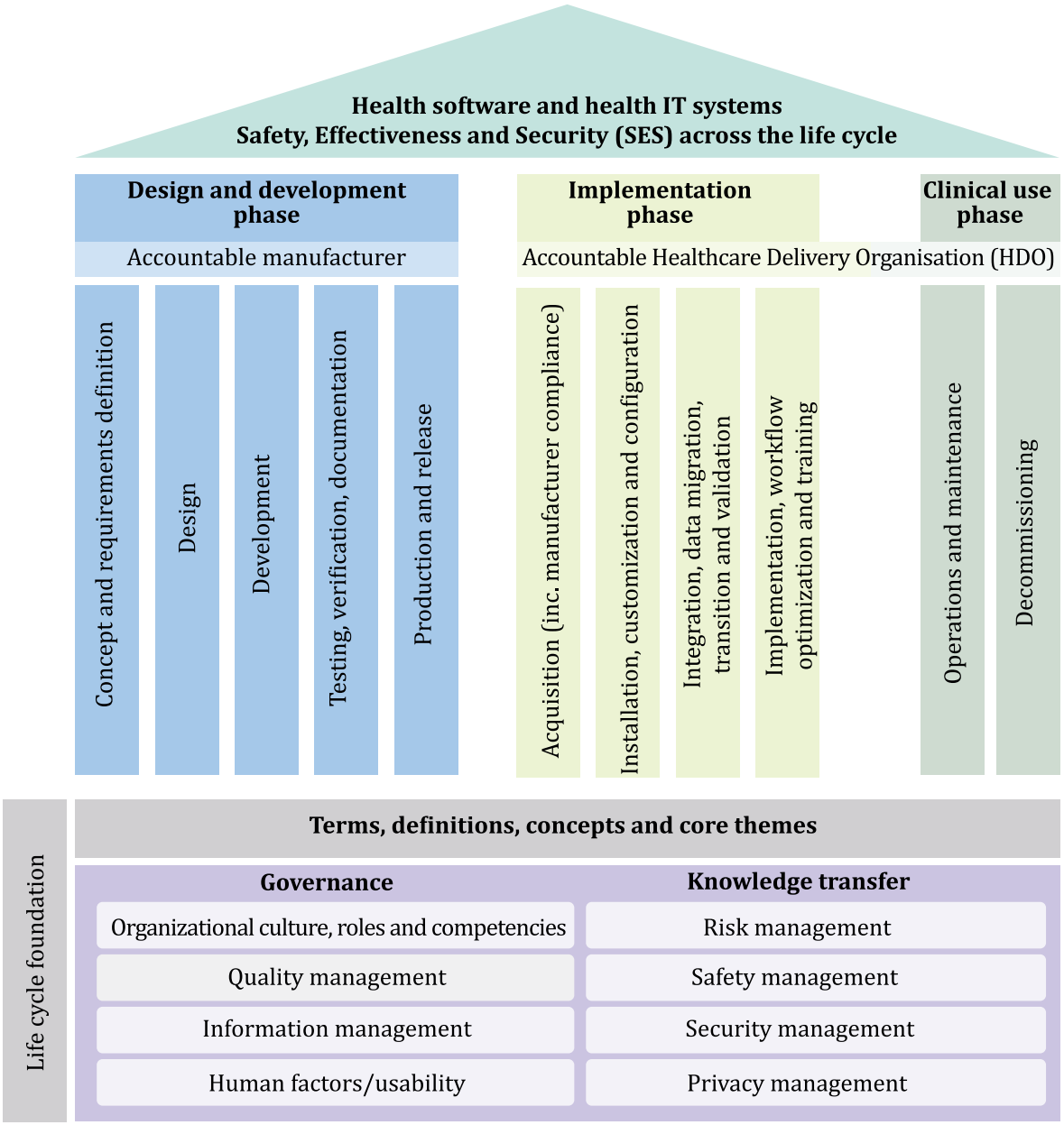


Figure 1 — *Life cycle* framework addressing *safety, effectiveness* and *security* of *health software* and *health IT systems*

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 of 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]

3.4.10
risk
combination of the probability of occurrence of *harm* (3.4.5) and the *severity* (3.4.20) of that *harm*

Note 1 to entry: The probability of occurrence includes the exposure to a *hazardous situation* (3.4.7) and the possibility to avoid or limit the *harm*.

[SOURCE: ISO/IEC Guide 63:2019, 3.10]

3.4.11
risk analysis
systematic use of available information to identify *hazards* (3.4.6) and to estimate the *risk* (3.4.10)

[SOURCE: ISO/IEC Guide 63:2019, 3.11]

3.4.12
risk assessment
overall *process* (3.2.10) comprising a *risk analysis* (3.4.11) and a *risk evaluation* (3.4.15)

[SOURCE: ISO/IEC Guide 51:2014, 3.11]

3.4.13
risk control
process (3.2.10) in which decisions are made and measures implemented by which *risk* (3.4.10) are reduced to, or maintained within, specified limits

[SOURCE: ISO/IEC Guide 63:2019, 3.12]

3.4.14
risk estimation
process (3.2.10) used to assign values to the probability of occurrence of *harm* (3.4.5) and the *severity* (3.4.20) of that *harm*

[SOURCE: ISO/IEC Guide 63:2019, 3.13]

3.4.15
risk evaluation
process (3.2.10) of comparing the estimated *risk* (3.4.10) against given *risk* criteria to determine the acceptability of the *risk*

[SOURCE: ISO/IEC Guide 63:2019, 3.14]

3.4.16
risk management
systematic application of management policies, procedures and practices to the tasks of analysing, evaluating, controlling and monitoring *risk* (3.4.10)

[SOURCE: ISO/IEC Guide 63:2019, 3.15]

3.4.17
risk management file
set of records and other documents that are produced by *risk management* (3.4.16)

[SOURCE: ISO 14971:2019 3.25]

3.4.18
risk tolerance
organization's (3.1.8) or stakeholder's readiness to bear the *risk* (3.4.10) after *risk control* (3.4.13) in order to achieve its objectives

Note 1 to entry: *Risk tolerance* can be influenced by legal or regulatory requirements.

[SOURCE: ISO Guide 73:2009, 3.7.1.3, modified — Replace risk treatment with *risk control*.]

3.4.19
root cause
set of conditions or actions that occur at the beginning of a sequence of *events* (3.4.2) that result in the initiation of a failure mode

[SOURCE: ISO 13372:2012, 8.9]

3.4.20
severity
measure of the possible consequences of a *hazard* (3.4.6)

[SOURCE: ISO/IEC Guide 63:2019, 3.17]

3.4.1.21
threat
potential for violation of *security* (3.2.13), which exists when there is a circumstance, capability, action, or *event* (3.4.2) that could breach *security* and cause *harm* (3.4.5)

[SOURCE: IEC Guide 120:2018, 3.16]

3.4.22
vulnerability
flaw or *weakness* (3.4.23) in a *system's* (3.3.17) design, *implementation* (3.2.6), or operation and management that could be exploited to violate the *system's security* (3.2.13) policy

[SOURCE: IEC Guide 120:2018, 3.18]

3.4.23
weakness
kind of deficiency

Note 1 to entry: *Weakness* can result in *security* (3.2.13) and/or *privacy risks* (3.2.9).

Note 2 to entry: Adapted from Reference [42].

4 Core themes

4.1 General

Information technology in healthcare is pervasive and continues to evolve in a complex and interconnected way. Consequently, the activities of all stakeholders become more interdependent as the scale of connected devices and interoperable *systems* grow. It is important that all of those involved understand the entirety of the *life cycle* of *health IT.* This is to ensure that they can plan and respond to any interdependencies and connections of which they were not previously aware. Therefore, formalized communication between these stakeholders is essential to maintain consistency in the management of *safety*, *effectiveness*, and *security* of the overall healthcare infrastructure.

Six core themes, as shown in Figure 2, provide the overarching basis for understanding how the eight foundational elements of the *life cycle* framework (in Figure 1) can be used to develop a cohesive and comprehensive approach to addressing *safety*, *effectiveness*, and *security.*

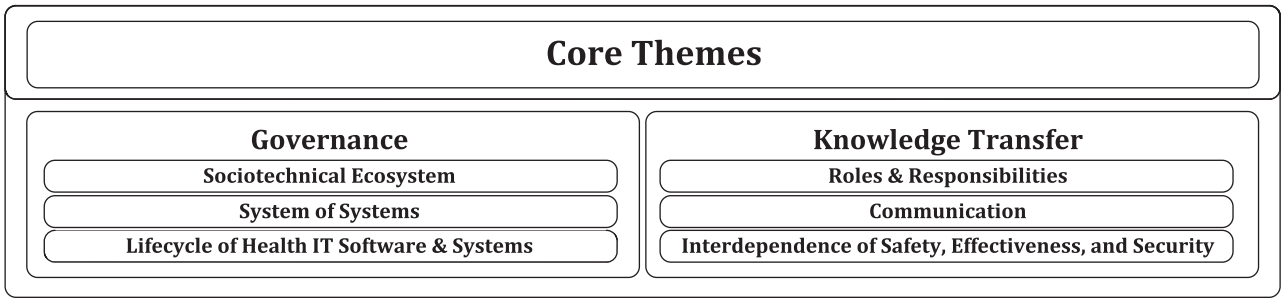


Figure 2 — Core themes

4.2 Sociotechnical ecosystem

The impact of a connected and complex healthcare ecosystem is not limited to the *health software* and *health IT systems*. It is important to consider the larger sociotechnical environment (Figure 3) and the potential impact to *safety*, *effectiveness*, and *security* that can arise in each part of the ecosystem and through the interaction of these parts. This ecosystem includes:

a) The *health IT infrastructure* (for example, hardware, software, networks, interfaces to other *systems*, *medical devices* and data), and the *organizations* involved in developing, implementing and operating the many *health IT components* and services,

b) The healthcare delivery context (for example, the clinicians, patients and other people involved, clinical workflow, and the specific *organization* setting where the *health IT system* is being deployed), and

c) The broader healthcare *system* (for example, regulations, funding and policy implications) within which the *HDO* (and its supporting *health IT systems*/infrastructure) must comply and operate.

NOTE This sociotechnical ecosystem exists within an external environment (for example, public opinion, ambient conditions), and therefore can also be subject to external influences.

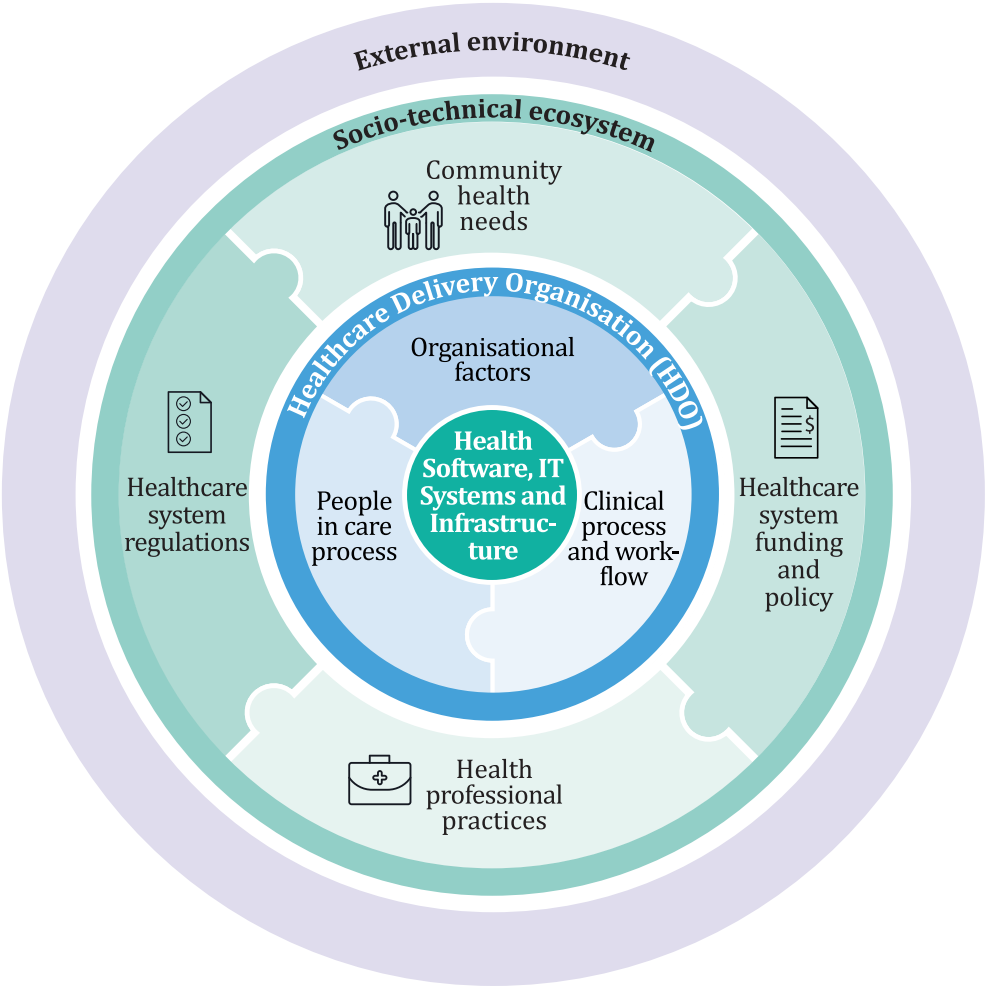


Figure 3 — *Health software* and *health IT systems* within their sociotechnical ecosystem

Given the scale of *health software*, *health IT systems* and *medical device* adoption in health care, research indicates that *safety* and *security* incidents involving the use of these technologies are under-reported. Both qualitative and quantitative research on reported incidents demonstrates that across this ecosystem the *root causes* of patient *harm* are diverse. Examples include errors and malfunctions in the software and underlying hardware, deficiencies in data *quality* and integrity, *security* and *privacy* breaches, faults in decision support algorithms, infrastructure failures, *interoperability* problems, record mismatches, errors in identifying patients, human-machine interface errors, poor alignment between *systems* and workflow, and inadequate training.

4.3 *System* of *systems*

In today's complex and integrated *health IT infrastructure*, the *life cycles* of the *health software*, *medical devices*, data and other *health IT components* are often interdependent. Each element of the *health IT infrastructure* has its own *life cycle*, with each *health IT system* and its subsystems adding at least one additional *life cycle*. Furthermore, each *medical device* that is integrated has its own *product life cycle* that follows a specific set of regulatory requirements for its safe and effective use. Adding to this complexity is the larger infrastructure of supporting core IT *components*, services and technology including networks, data centres, and middleware.

It is important to ensure that the *life cycle* management *processes* work together to deliver an effective clinical experience for each patient. Figure 4 highlights the '*system* of *systems*' complexity by illustrating the interdependence of the diverse elements in a typical *healthcare delivery organization's health IT infrastructure*. It also demonstrates the range of external connections to the internet, *cloud services* and other *organizations* that are often involved.

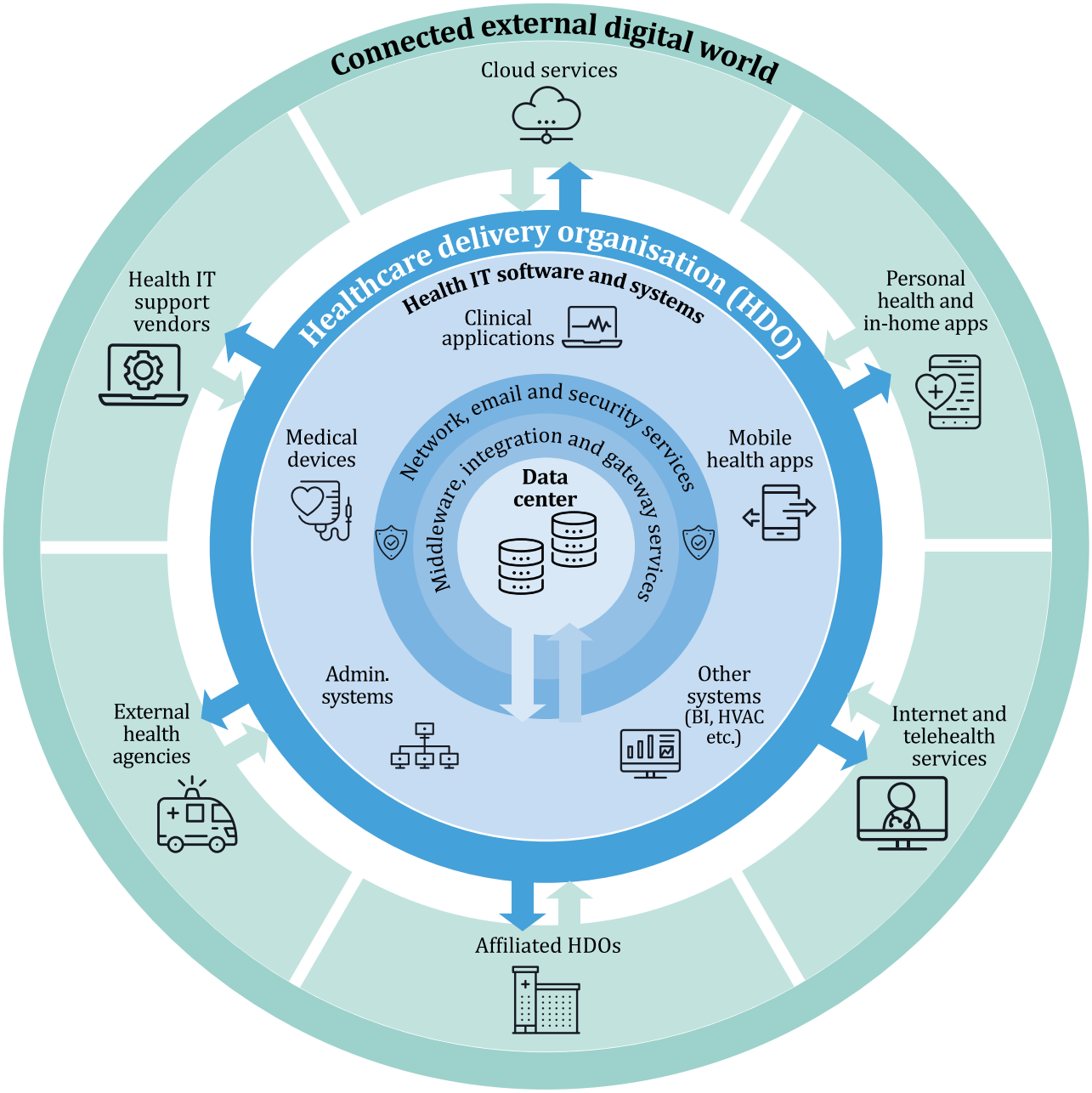


Figure 4 — *System* of *systems*

4.4 *Life cycle* of *health software* and *health IT systems*

The *life cycle* of *health software* and *health IT systems* involves many stages and involves several distinct *roles* and responsibilities (described in 4.5). All *roles* and responsibilities need to work together in sharing responsibilities for optimizing *safety*, *effectiveness* and *security*.

Although each *life cycle* can vary, the stages are similar and can conceptually be broken down into a set of activities. This applies to both the full life cycle and the continuous maintenance sub-cycle loop, as outlined in Figure 5.

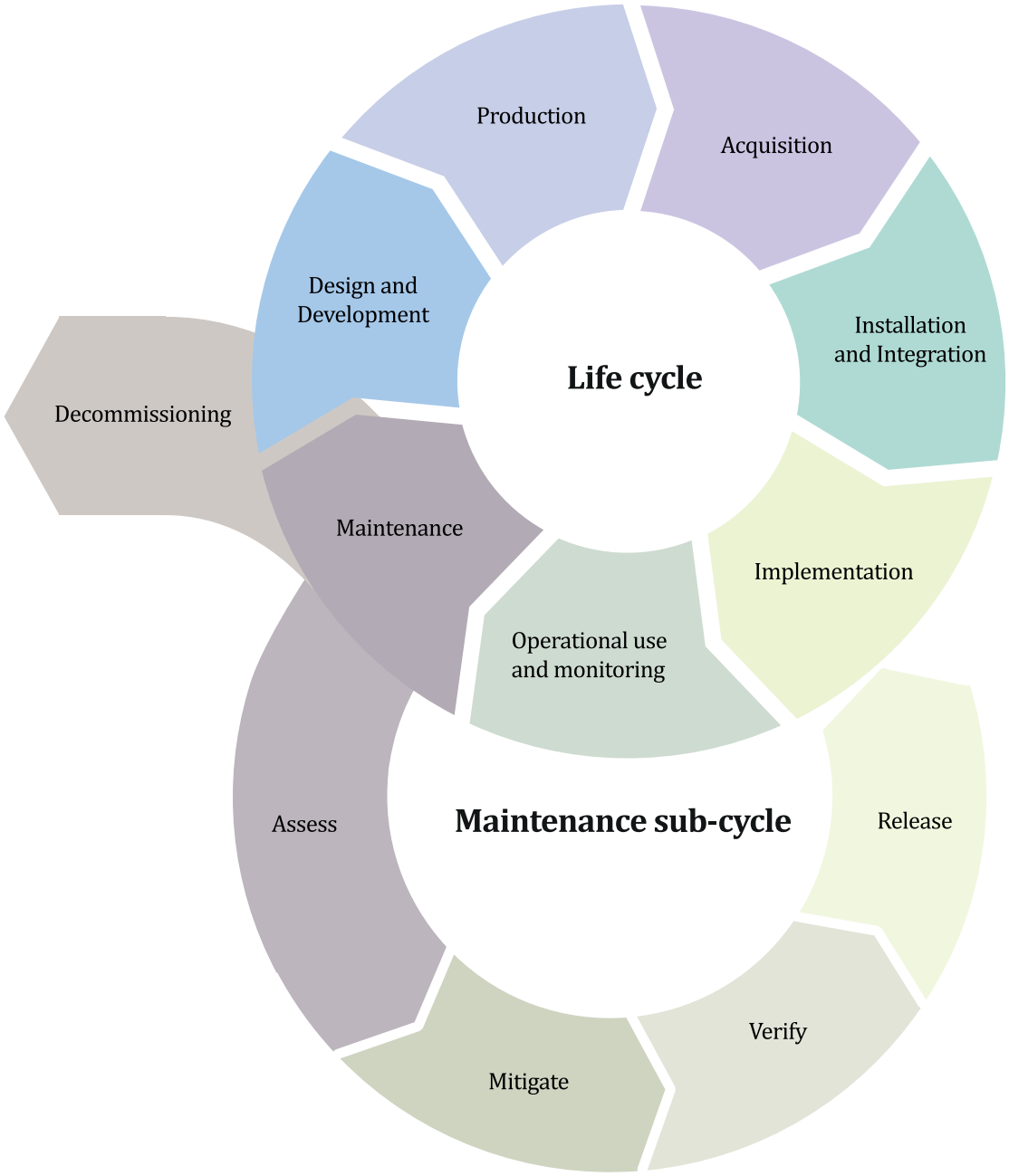


Figure 5 — *Life cycle* stages – *Health Software* and *Health IT Systems*

Health software and *health IT systems* often evolve in an agile, iterative, or recursive way and can range from large *cloud computing* solutions to much smaller *health IT components* (for example, personal health apps available through an online store). While the scale may differ, the *health IT components* and *systems* can iterate frequently and with almost continuous cycles of development, to address software maintenance, changing business needs and *customer* expectations. The frequency of the maintenance and design/development cycles, and the degree to which stages such as 'acquisition' are required, also differ depending on the specific health software and health IT system, its sociotechnical ecosystem and the degree of adaptive change required over its life. Within this ecosystem, processes such as *change-release management* and *configuration management* are very important.

The *health IT infrastructure* and each *health IT system* and *health IT* sub-*component* within the '*system* of *systems*' has its own *life cycle* so there are multiple overlapping *life cycle*s occurring at any one time for the following:

a) *Health IT systems*, software and their *components*;

b) *Medical devices* and their associated software and hardware;

c) End-user workstations, tablets, smartphones and other access devices;

d) IT networks, interfaces and *security* subsystems;

e) Supporting general purpose IT including hardware and software;

f) Data, information and supporting terminology, algorithms and coding *systems*.

As an example, the software on a network switch has its own *life cycle*, as does the hardware that the network switch is made of, as does the infrastructure on which the network switch is placed, and so on.

Figure 6 illustrates how a *health IT infrastructure* is composed of a diverse set of *systems* that are interconnected to share data, that interoperate and use common infrastructure. Each *system* is typically composed of multiple *health IT components*, which are themselves composed of data and multiple sub-*components*, each of which has its own *life cycle*.

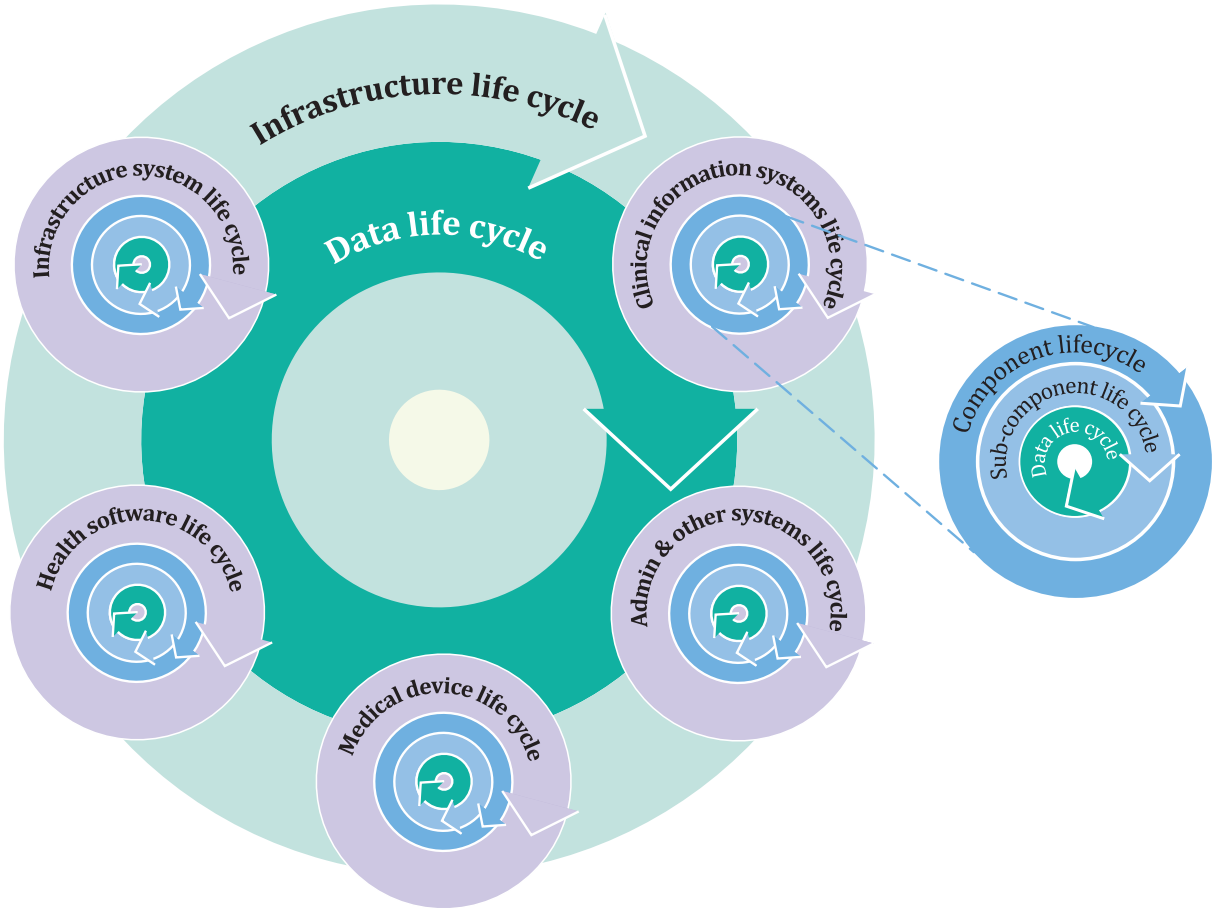


Figure 6 — *Life cycles* within *life cycles*

Each set of data also has a *life cycle*. Data is created, used, and can be recompiled with other data to create new data sets. If not managed properly, the source of the data can be lost and therefore the integrity of the data can be difficult to verify. Data integrity is an essential element of *security*, and if data is not properly managed and maintained across its *life cycle*, it can have serious impact on *safety* and *effectiveness*. Techniques, such as master data management and metadata management, are especially valuable for healthcare information to adhere to authorization, consent and other *privacy* principles. Further, data that is collected in multiple care settings and then integrated and transformed into information where accuracy is critical to patient care decision-making, also needs appropriate management.

4.5 *Roles* and responsibilities

The responsibility for *safety*, *effectiveness*, and *security* is shared across many *roles* (see Table 1).

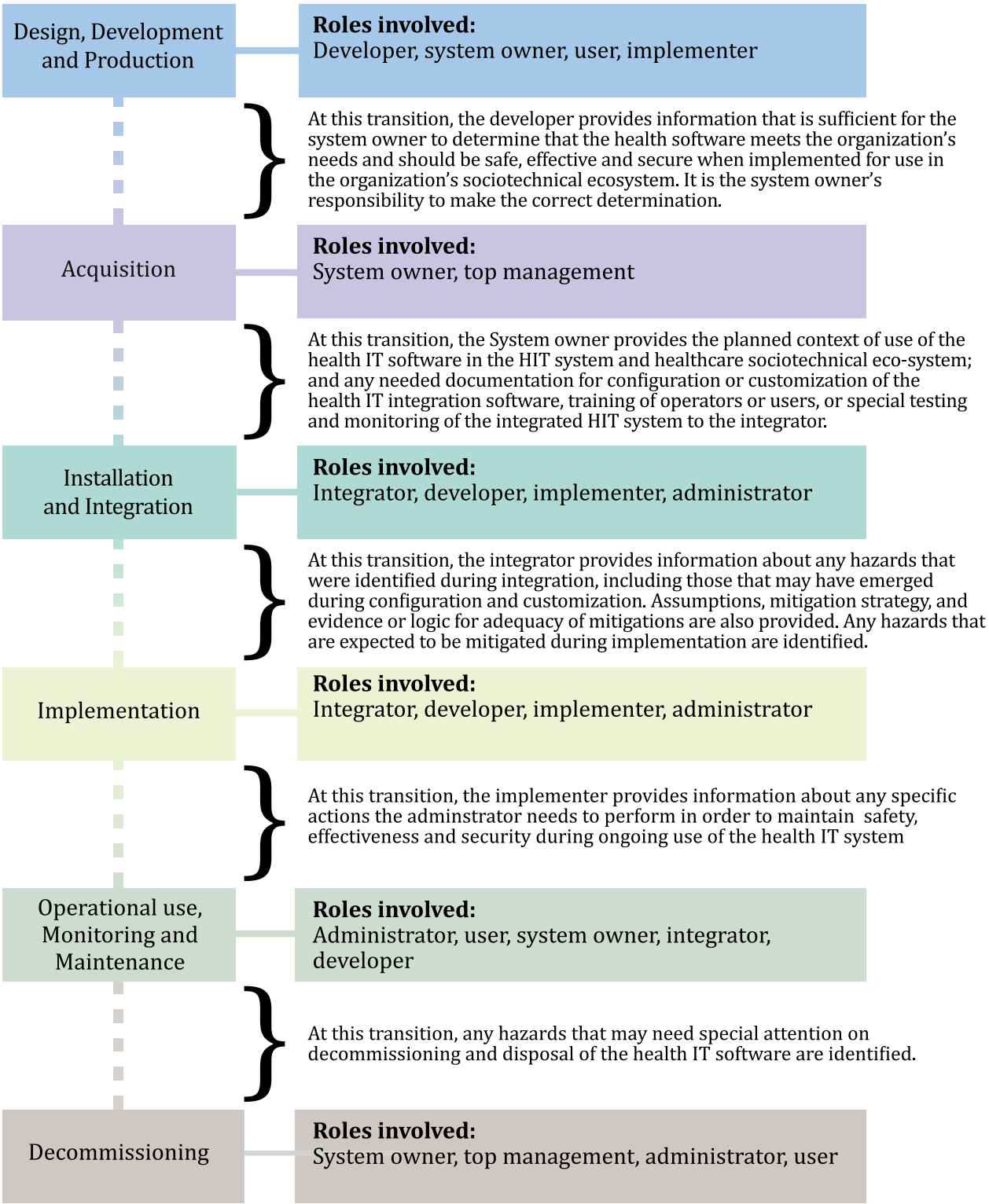
Table 1 — *Life cycle roles*

Role	Description
Top management	Group of people who direct and control an *organization* and have overall accountability in an *organization*.
System owner	Senior executive accountable for ensuring the *health software* and *health IT system* being acquired and implemented will meet their *organization's* healthcare delivery services needs for its *intended use*.
Developer	Entity responsible for execution of the design and development phase (from concept through to release and maintenance) of a *health software* or *health IT system*. NOTE A *developer* could be part of a *manufacturer organization*, a supplier of services or an *HDO* for example.
Integrator	Entity responsible for incorporation of components into the *health IT infrastructure* used by the *healthcare delivery organization*, including technical installation, configuration, and data migration
Implementer	Entity responsible for the clinical installation, workflow optimization and training in the clinical setting (an *implementer* can be the *developer* or owner).
Administrator	Person with *role* responsible for the ongoing operation of the implemented health IT system and ensuring it is safeguarded and maintained on an ongoing basis.
Users	Persons using the *system* in the clinical setting, which can include, for example, consumers in the case of personal health records.
NOTE Adapted with permission from Reference [38].	

These *roles* are not specific to an *organization* type. For example, while hospitals can integrate, implement and operate the *systems* they use, they can also choose to internally develop their own software, and therefore play multiple roles. Similarly, *medical device* companies and *health software* and *systems manufacturers* can serve as *integrators*, *implementers*, or *administrators* (as in the case of cloud-based software) of the *systems* they develop. Where a *system* has multiple *health IT components*, a different *organization* can be responsible for different aspects of the *system*. For example, a hospital can contract-out certain aspects of its IT operations such as network or server operations to a third-party *cloud service* provider.

The assignment of responsibilities for managing the *key properties* of *safety*, *effectiveness*, and *security* within an *organization* is not necessarily reflected in a dedicated job title but can be included as specific responsibilities formally held by an individual. In some cases, specific activities in a *role* can be split between various individuals, depending on the structure of the *organization* and, in some cases, the specific *health IT component* or *system* in question.

Figure 7 provides an overview of the relationship between *roles*, *life cycle* stages, and transition points where transfers of responsibility occur and where information is shared to provide continuity in managing the *key properties*.



NOTE Adapted with permission from Reference [38].

Figure 7 — *Health software roles*, *life cycle* stages and transition points

4.6 Communication

Communication across transition points in the *life cycle* is important to any managed *process* and it becomes vital in complex *systems* with diverse stakeholders. As *health software* and *health IT systems* pass through different stages in their *life cycles*, there is important information that, when shared,

significantly enhances the management of the foundational elements between and across the many roles and organizations involved.

At each stage of the *life cycle*, it is important that *organizations* with *roles* responsible for managing aspects of *safety*, *effectiveness*, and *security* are clearly identified. As *health software and health IT systems* move through their *life cycle* stages (see Figure 8), these *organizations* need specific information from earlier *life cycle* stages to properly assess and manage the *safety*, *effectiveness*, and *security* in carrying out their *roles*. Additionally, they can share information for maintenance and monitoring to *organizations* with *roles* involved in other stages of the *life cycle*.

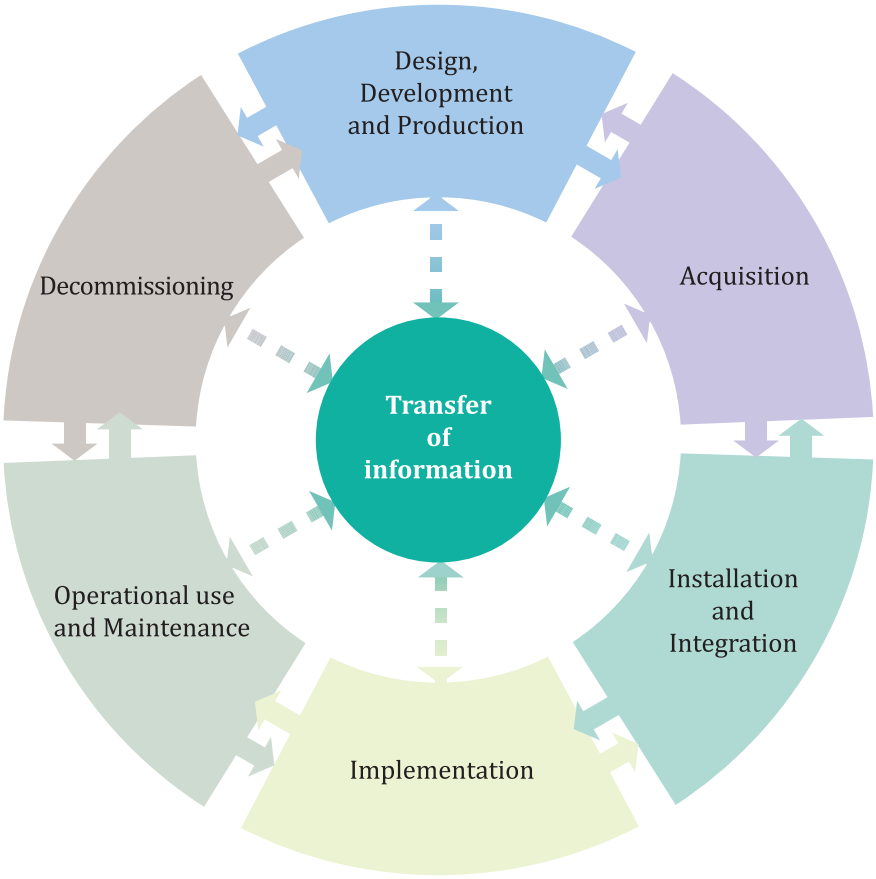


Figure 8 — Transfer of information at transition points in a continuous communication

There are three important issues to address when creating communication plans:

a) what information is to be communicated;

b) who will receive and who will transmit the communication;

c) how best to communicate the information.

In many cases, *roles* at different stages in the *life cycle* also need to receive information back into their *process*. For example, when a *medical device manufacturer* sells a *medical device* to a *customer*, that *manufacturer* is expected to monitor the post market performance of that device, collect feedback from *customers*, and reassess the *risk* of issues that occur in the field. In some cases, this information can initiate the need to revise the device to help maintain the *safety*, *effectiveness*, and *security* of that *medical device*. In the other direction, the *manufacturer* would be expected to communicate forward to the *customer* if additional *risk control* measures or a change is necessary and, in some cases, carry out a formal recall to make a correction to devices in the field. Similar needs for communication exist for *health software* and *health IT systems* given the number of *roles* and transition points involved. As depicted in Figures 7 and 8, this communication can involve multiple parties and stages.

It is important that this transfer of knowledge and information is sufficiently formalized and predictable so that different stakeholders can communicate in a timely and effective way across *life cycle* stages and between *roles*. One method to formalize this communication and information transfer is to use an *assurance case*. An *assurance case* can be used to communicate information and knowledge about different *risks* to other *roles*. This methodology is explored further in Annex C.

Another method is *responsibility agreements*, in which stakeholders specify which tasks are the responsibility of a specific party. In some cases, these responsibilities are time-bound and expire after a certain time.

Accompanying information and labelling is another type of communication that helps to deliver specific information from a *manufacturer* to a *customer*. Labelling can be particularly important for connected and interoperable *systems*, where *manufacturers* can communicate non-standard interface requirements and characteristics, functional and performance requirements, and the purpose of the electronic interface. This can be critical information for *integrators* and *implementers* to have from the *manufacturer* to ensure that the device performs as intended.

Another important avenue for communication is the retrospective reporting and management of *safety* and *security* incidents, including near misses. This involves communication between different *roles* at the operational level (e.g. supporting IT units, service contractors and affected clinical departments) as well as *manufacturers* of health software, *health IT system* and infrastructure *components*, regulators and agencies involved in aggregating case reports.

4.7 Interdependence of *safety*, *effectiveness* and *security*

The same *risks* (and their *risk control* measures) can impact *safety*, *effectiveness* and *security*, and it is important to recognize the interdependence of these three key properties in assessing and managing these *risks* and their *risk control* measures (Figure 9). For example, a *risk* that *systems* or data will not be available at the point-of-care is not only a *security risk*, it can have significant impact on *safety* if patient care decision-making is compromised, as this can impact the *effectiveness* of the *system* (and its benefits) by jeopardizing clinician confidence in using the *system* as a clinical tool.

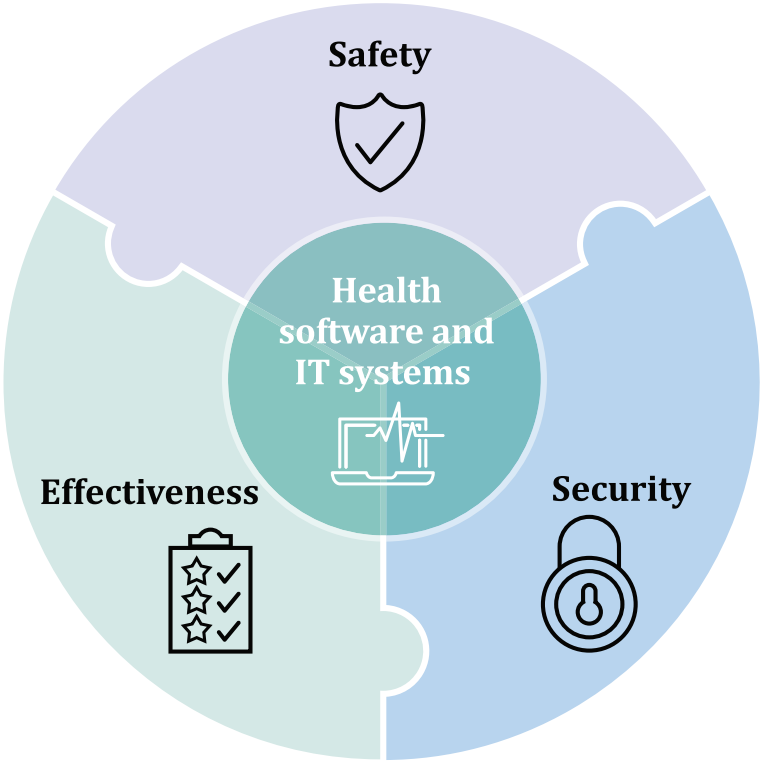


Figure 9 — Interdependence of *safety*, *effectiveness* and *security*

A consequence of the interdependence of the *safety*, *effectiveness*, and *security* properties is that well-intended *risk control* measures of certain *risks* can adversely impact one or both of the other properties. For instance, adding controls to reduce the *risk* resulting from unauthorized access, can impact *system usability* and availability and hence compromise *system effectiveness* (and benefits realization). It can also result in *system* workarounds which adversely impact *safety*.

In addressing *safety*, *effectiveness*, and *security risks*, and achieving the intended benefits to support continued investment in *health software* and *health IT systems*, a comprehensive approach is key to optimizing the synergies and balance across the three properties. It is important to ensure that the *effectiveness* of the *system* (its aggregate benefit) always outweighs the *residual risks* involved in its *implementation*.

5 Foundational elements

5.1 General

The *life cycle* framework addressing *safety*, *effectiveness* and *security* of *health software* and *health IT systems* has eight foundational elements (Figure 10), which support the six overarching themes (Figure 2) as articulated in Clause 4. These eight elements inform the stakeholders across the *health software* and *health IT systems life cycle* on how to address *safety*, *effectiveness*, and *security* in an integrated and informed way. The foundational elements are grouped into two categories – Governance and Knowledge Transfer.

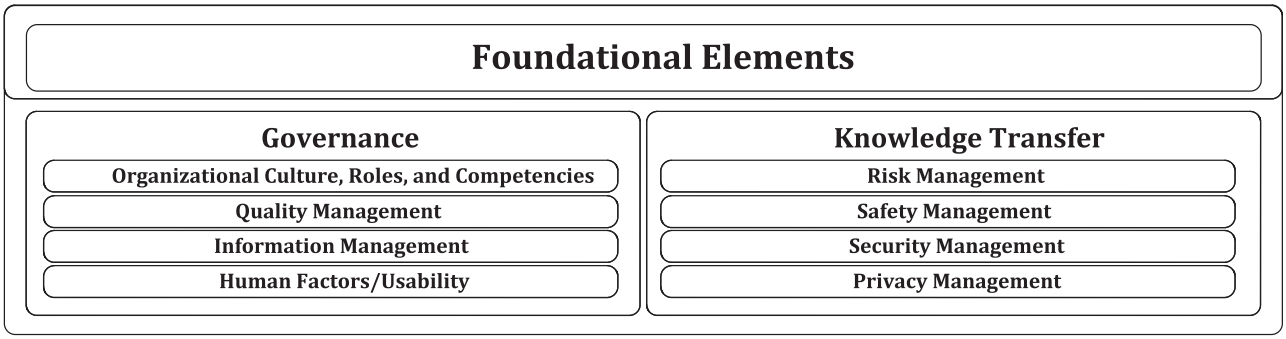


Figure 10 — Foundational elements

Governance comprises four foundational elements involving activities that are typically the responsibility of each stakeholder *organization*, yet are critical to achieving *safety*, *effectiveness*, and *security* at all *life cycle* stages. These elements should be addressed in the governing structure of *manufacturers*, *HDOs*, and other supporting *organizations*, and used by these *organizations* to maintain the *key properties*. The application of these elements within organizations will vary depending on the type of stakeholder and the life cycle stage.

Knowledge Transfer comprises four foundational elements that are important at the enterprise level, but also involve communication across *organizations*, *roles* and *life cycle* stages. From the *manufacturer* or *developer* perspective, this category of elements involves many activities that evaluate *risks*. These activities produce information that is important to designing and maintaining *products,* as well as communicating a subset of this information to those who acquire the *products*. From the *HDO* perspective, the *roles* involved will then continue the communication of this essential information to help guide the integration, *implementation*, use, and decommissioning of these *products* later in their *life cycle*. This information is integrated into enterprise-level *risk*, *safety*, *privacy*, and *security* management *processes* that are in place to manage the activities at each stage and by each stage owner. Information can be communicated in different ways. One way to organize and transfer information is by the use of *assurance cases*. Annex C shows how information can be captured and communicated using *assurance case* reports.

5.2 Governance (intra *organization* focus)

5.2.1 General

Figure 11 shows the four foundational elements related to Governance.

Figure 11 — Foundational elements – Governance

5.2.2 *Organization* culture, *roles* and competencies

5.2.2.1 Statement

Given the critical *role* of people in the delivery of healthcare and *health IT systems*, leadership by *top management* is key to establishing a culture of *safety*, *effectiveness* and *security.* Within this culture, staff are appropriately skilled to fulfil their *roles* throughout the *life cycle* of health software and *health IT systems*.

5.2.2.2 Rationale

Studies[43][44][45][47] of *health IT safety* and *security events* emphasize the importance of the organizational and human dimensions of the ecosystem in which *health IT systems* are developed and implemented. Since there are many causes of potential error and many parties involved across the *system life cycle*, developing a culture of *safety*, *security* and continuous learning in *organizations* is vital, similar to the way it has been nurtured in industries such as aviation. In healthcare, the evidence on safety culture and clinical metrics indicates that perceptions about teamwork, *safety*, and leadership correlate with the *quality* and safety of care. For instance, the US Veterans Health Administration *system's* teamwork training programme was shown to decrease surgical mortality by 18 %, improved safety culture scores, resulted in better operational and clinical *process* metrics, and significantly reduced *harm*[47].

5.2.2.3 Key concepts and principles

Top management establishes an organizational environment conducive to *safety*, *effectiveness* and *security* by the following:

a) committing to proactive measures to assess, avoid and control *risks* through good *processes* and competent staff, who are supported in maintaining and advancing their skills to manage these *risks*;

b) acknowledging the *risks* of an *organization's* activities and demonstrating their determination to achieve consistently safe, effective and secure operations;

c) consistently emphasizing the importance of *safety*, *effectiveness* and *security* so that everyone across the *organization* sees these as their individual (and collective) responsibility;

d) establishing a blame-free environment where individuals are able to report errors or near misses without fear of reprimand or punishment;

e) designating a focal point for *safety*, *effectiveness* and *security* at the senior management level, and defining the responsibilities of staff in managing these across the *life cycle*;

f) fostering collaboration and *user* engagement across all levels of the organisation and disciplines (including IT, clinical engineering and care delivery) throughout the *life cycle* to identify *risks*, design solutions and respond to patient *safety*, *effectiveness* and *security* problems;

g) providing sufficient resources and assigning competent personnel from each of the specialist areas involved in developing and assuring *health software*, *health IT systems* and data;

h) ensuring that the level of resources provided is commensurate with the scale and complexity associated with the *system* under consideration, with additional resources available to address emerging *safety*, *effectiveness* and *security* concerns on a priority basis;

i) designating who is responsible for authorising release of the *health IT system* for subsequent deployment in live service and approving the associated documentation supporting the *safety*, effectiveness and *security* of the *health IT system*;

j) regularly reviewing the overall performance of the *processes*, policies and capabilities in managing the *organization's safety*, *effectiveness*, and *security risks* effectively, considering new and emerging *threats*, organizational restructuring and staff changes, service and contractual provisioning, etc.;

k) implementing and maintaining policy that includes a commitment to satisfy legal, regulatory and legislative requirements.

A culture of *safety* involves continuous communication, education and awareness building involving continuous monitoring, documentation and analysis.

Assigned resources require the education, training and time to apply the level of effort and skill necessary to carry out *safety*, *effectiveness* and *security* activities in a robust and competent manner.

Safety and *security management* is an integral part of all *health IT* projects and activities, and should be built into *health IT processes*, competencies and training. Formal review, prior to the release of a *health IT system*, involves sign-off by appropriate individuals in the *organization* to ensure the properties of *safety*, *effectiveness* and *security* have been adequately addressed.

Ongoing monitoring, reporting and incident management *systems* are important post-*implementation*. All incidents, including near misses, are a continuous improvement opportunity through the collaboration of all staff involved.

5.2.2.4 Approach

A multi-dimensional approach to *safety, effectiveness* and *security* includes the following:

a) Educating *health IT* staff about *safety* and *security risks* and developing their competencies in identifying and managing the *risks* in their day-to-day work;

b) Ongoing organizational commitment of resources to enable the *organization* to anticipate, respond and address *safety*, *effectiveness* and *security* concerns;

c) Supporting appropriate clinician engagement at all stages of the *life cycle* for clinical *systems*, including senior clinical sign-off at designated checkpoints, before new or modified *systems* are implemented;

d) Fostering staff vigilance and collaboration in identifying *safety*, *effectiveness* and *security* issues within a culture supportive of continuous improvement and collective responsibility for solutions;

e) Establishing an open and integrated approach to managing the *key properties* of *safety*, *effectiveness* and *security* across the *system life cycle* within the *organization,* and fostering collaboration and sharing knowledge about *safety*, *effectiveness* and *security* concerns with other *organizations*.

5.2.3 *Quality* management

5.2.3.1 Statement

Quality management is concerned with the degree to which an *organization's* objective(s) are consistently being met, including *customer* expectations for example.

5.2.3.2 Rationale

In healthcare, the overarching objective is to improve the health of the patient, and *quality* is a key focus for many *processes*, particularly clinical programme objectives that are enabled by *health software* and *health IT systems*. *Effectiveness* is a *key property*, and *quality* management *processes* are important in achieving *quality* outcomes and meeting *customer* expectations for effective *health software* and *health IT systems*. *Quality* management also supports *safety*, *effectiveness* and *security* as *quality management processes* enhance the *quality* of the *systems*, *processes* and people that make up the *system* and its sociotechnical environment.

5.2.3.3 Key concepts and principles

Quality management is concerned with ensuring that *processes* consistently yield the intended results.

Across the *life cycle* of *health software* and *health IT systems*, *quality* has two complementary dimensions:

— *Process quality* — relating to the *processes* associated with the development, *implementation* and operation of *systems*.

— *Data and information quality* — relating to the *quality* of data (and its transformation into information) used by clinicians and health administrators to make decisions including diagnosis, treatment, care, resource allocation and other matters affecting the patient or client.

Quality management involves four main aspects:

Quality Planning	Quality Assurance
Quality Control	Quality Improvement

Key principles of an effective *quality* management programme include the following:

a) *Customer* focus — understand current and future *customer* needs, meet *customer* regulatory, policy and organizational requirements and strive for continuous improvement;

b) Leadership — establish a unity of purpose and direction for the *organization* and an internal environment that fosters staff engagement;

c) *Process* approach — manage activities and related resources as a *process* to achieve desired results;

d) *Systems* thinking — identifying, understanding and managing interrelated *processes* as a *system* to achieve objectives;

e) Continual improvement — to further performance goals;

f) Factual approach to decision making — based on the analysis of data and information;

g) Mutually beneficial supplier relationships — An *organization* and its suppliers are interdependent.

5.2.3.4 Approach

Administrators and *users* of *health IT systems* rely on *developers* and *implementers* to provide *quality products* and services. *Developers*, *implementers* and patients also rely on healthcare *organizations* and healthcare professionals to use *quality* management *processes* to implement, operate and use the *health IT system* in a safe and effective manner.

Standards providing further guidance include ISO 9000 and ISO 9001 for quality management; the ISO/IEC 20000 series on service management; and ISO 13485 for medical devices.

5.2.4 Information management

5.2.4.1 Statement

Information is the lifeblood of healthcare delivery and proper governance is critical to ensuring collective responsibility (and trust) in the collection and appropriate use of high-*quality* information.

Information management is the set of multi-disciplinary structures, policies, procedures, *processes* and controls for managing information at an enterprise level, supporting an *organization's* immediate and future regulatory, legal, *risk*, environmental and operational requirements.

5.2.4.2 Rationale

Deficiencies in the accuracy and availability of patient information are a major contributing factor in *safety* incidents. Therefore, a comprehensive information management framework is essential to reduce *risks* and manage incidents where information deficiencies are a *root cause*. Situations where *health software* and *health IT systems* provide information that is erroneous, and errors are not easily detected by the clinician (for example due to data mapping, algorithm or logic errors), are particularly important from a patient *safety* perspective.

The *role* of data in the safe, secure and effective operation of *systems* is just as important as that of hardware and software. The data and information involved can have multiple *life cycle*s that need to be managed (for example, when data is integrated from multiple sources and transformed into information supporting clinical decision making). The *hazards* associated with *health IT systems* that are built and assured to even the highest standards will, to some extent, depend on the data contained in them, such as blood group or allergy status. If these data are erroneous, the consequences might be more severe than a hardware or software failure. This is an issue with *systems* that typically store health-centric data used to inform clinical decisions. *Systems* are no longer merely productivity tools; they are increasingly depended on for clinical decision making. It is no longer safe to assume that healthcare providers will detect errors in such vast stores of data.

Effective information management also supports *privacy* and *security* by engaging leaders across the *organization* to develop and communicate overarching *privacy* and *security* policies.

5.2.4.3 Key concepts and principles

Information management needs to be mandated and resourced at the organizational level, engaging all stakeholders with a key stake in the collection, processing and use of health information. Information management includes the following:

a) Information custodianship and accountability;

b) Information management policies and *processes*;

c) *System* access policy;

d) Openness and transparency;

e) Data and metadata documentation;

f) Master data management;

g) Accuracy and data *quality*;

h) Data retention, archiving and disposal;

i) Data flows and data sharing agreements;

j) Compliance and auditing to established policies.

5.2.4.4 Approach

Information management policies should be mandated at the organizational level, accompanied by an education and awareness programme. It is important that these policies are valued by the organization and embedded into the culture of the organization.

Organizations with responsibility for data should have a clear understanding of the associated *risks* in order to identify the level of effort required to addressing them. *Safety* and *security* are major reasons for investing effort in managing data and information across its *life cycle*.

Data *quality* shall be continually monitored and managed across all data *quality* dimensions – including accuracy, completeness, comparability, relevance, reliability, timeliness and accessibility.

Appropriate data stewardship involves policies, controls, cross-*organization* engagement, training and awareness.

The transformation of data into information informing care decisions is particularly challenging in health care since data is collected at various points in the care delivery *process*, often by different *organizations*. Techniques such as master data management and metadata are important in ensuring that data is correctly collated and transformed by staff with information management and clinical expertise. This is to ensure that *health IT systems* integrate, transform and present data and information to support its safe, effective and secure use for the *intended purpose*.

5.2.5 Human factors and *usability*

5.2.5.1 Statement

Human factors and *usability* account for human strengths and limitations in the design of interactive *systems* involving people, tools and technology, and work environments.

5.2.5.2 Rationale

Health IT systems are frequently implemented in complex sociotechnical ecosystems, where failure to properly address human factors and *usability* can compromise patient *safety*, *effectiveness* and *security*.

Highly usable *health software* and properly implemented *systems* contribute to safer healthcare through addressing human factors and *usability*, such as decreasing the cognitive load on *users* and integration into clinical workflow.

5.2.5.3 Key concepts and principles

Human factors and *usability* engineering consider physical demands, skill demands, mental workload, workflow impacts, team dynamics, and aspects of the work environment and the *system* design and human interface that are required to complete tasks safely and effectively.

Healthcare is often provided in a busy and intense environment, where the cognitive load imposed by a new *system* needs to be carefully considered and controlled.

Health IT systems usually necessitate changes in clinical and business workflows. A comprehensive clinical *change management process* (Figure 12) will ensure appropriate clinical and business input into designing, monitoring and optimizing the *process* (including a suitable post-*implementation* period to maximize *effectiveness* and minimize *safety* and *security risk*).

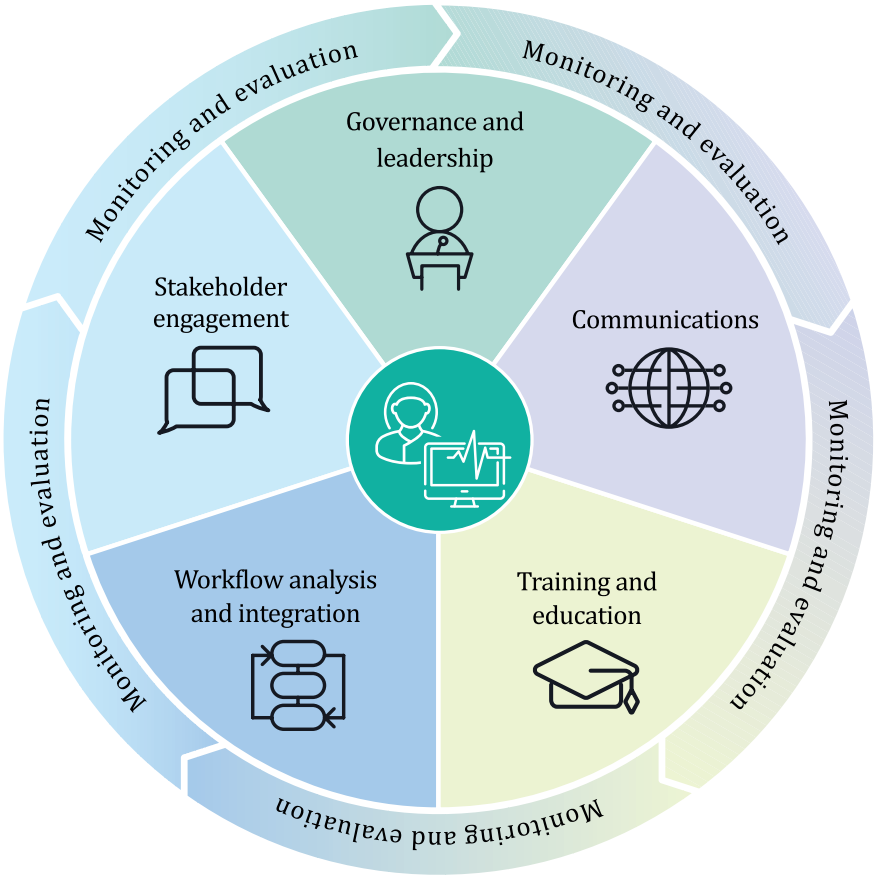


Figure 12 — Addressing the human element through clinical *change management process*

Strong leadership, cross-sectional *user* engagement, and communication is necessary from design through to *implementation*, given the increasing complexity of *health software* and *health IT systems*, together with the unique features of local sociotechnical ecosystems that they are being implemented into. Human factors and *usability* should be addressed at all stages of the *life cycle* and subsequently monitored and evaluated in real-life deployment, pre- and post-*implementation*.

Hazards due to human factors and *usability* factors should be assessed and *risks* controlled in accordance with their expected impact. *Risks* of patient misidentification, errors in using decision support tools or incorrectly interpreting key clinical information, should be managed very carefully.

Workflow analysis is a vital technique in properly integrating the new *health IT system* into *users*' clinical *processes* and work environment. At the point of *system implementation*, a comprehensive approach to training and support for *users* can further reduce the *risk* of use errors and lessen barriers to *system* adoption and *effectiveness*.

Use of complex clinical *systems* usually evolves over time as *users* adapt to the *system*, make appropriate adjustments to their workflow and learn to use the new *system's* more advanced functionality. Ongoing monitoring and *user* support as an element of clinical *change management* is important in reducing errors and *safety* incidents, as well as in optimizing care *quality* and *effectiveness*.

5.2.5.4 Approach

User-centred design is an important approach in the design of new *systems* and care needs to be taken to observe and then test design solutions in an appropriate number of situations that emulate the actual clinical environment.

Just as *user*-centred design is important in the early stages of the *life cycle*; a comprehensive clinical *change management* and training strategy can control many of the *risks* at the *implementation* stage.

Since human factors and *usability* issues are not always obvious at the time of design and *implementation*, regular observation and surveillance are important to identify new concerns. Supporting and fostering a culture of continuous improvement and learning in the work environment through clinical *change management* and training is also valuable in optimizing safe, secure and effective use of *systems*.

5.3 Knowledge transfer (inter- and intra- *organization* collaboration)

5.3.1 General

Figure 13 shows the four foundational elements related to knowledge transfer.

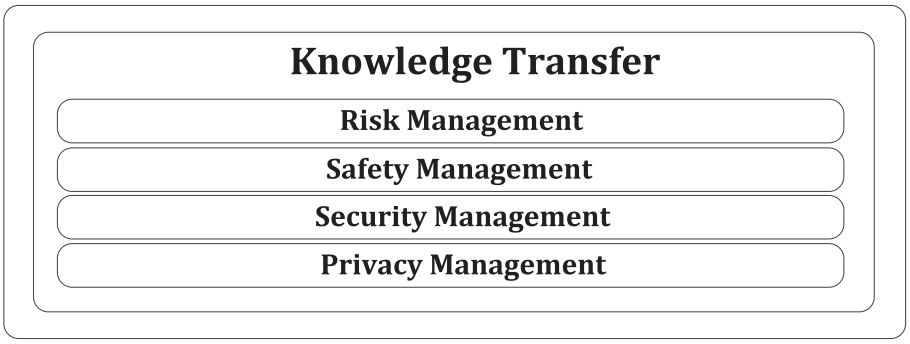


Figure 13 — Foundational elements – knowledge transfer

5.3.2 *Risk management*

5.3.2.1 Statement

Risk management is the *process* of identifying, assessing, controlling, and monitoring *risks*. For the purpose of this document, *risks* are related to injury or damage to the health of people, or damage to property or the environment. While broader enterprise *risks* such as cost, schedule, and uncertainty in achieving objectives are not specifically addressed in this document, damage to the *organization's* reputation is relevant if it impacts *safety*, *effectiveness* and *security* (for example by undermining patient and healthcare provider trust in using the *system*).

5.3.2.2 Rationale

Health software and *health IT systems* enable important benefits and efficiencies in healthcare delivery and outcomes but can also introduce new *risks*. These potential *risks* shall be identified, managed and minimized (mitigated).

Risk management is therefore an important and integral part of *safety*, *security* and *privacy* programmes, as it provides the methodology to identify and evaluate conditions that can lead to patient *safety*, *security* and *privacy* incidents, as well as to assess and select *risk control* strategies to reduce, transfer or eliminate these *risks* to an acceptable level.

5.3.2.3 Key concepts

At a high level, *risk management* activities can be framed using four questions:

1) What is the *intended purpose* of the software or *system*?

How the software or system is used impacts *risk* — for example, an analytics tool that examines clinical patient records for billing purposes has a different *risk* profile than a similar tool used to suggest alternative patient therapies.

2) What can go wrong?

Once the *intended purpose* is clearly defined, potential *risks* can be identified, analysed and evaluated. For example, is there potential to duplicate patient records that could result in over-medication of a patient? Reasonably foreseeable misuse is also important to consider.

3) What can be done about it?

Once unacceptable *risks* have been identified, they are documented, and *risk control* strategies are implemented to reduce the *risk*. For example, the software for medication order entry can have a control added that checks to see if the same prescription has been written for that patient in the last 24 hours. *Risks* are expected to be reduced as low as practicable. Alternately, a decision can be made to accept the *risk* without further *risk control* if the *risk* is acceptable.

4) Are the controls effective?

Simply documenting and implementing *risk control* measures is not sufficient. It should be continuously demonstrated that the controls are effective in addressing *exposures* and reducing *risk*, and that the *risk controls* do not introduce new *risks*. The efficacy of the *risk control* measures should be *verified,* and a further *risk evaluation* performed to ensure that the *risk controls* do not negatively change existing *risks* or introduce new *risks*.

An effective *risk management* programme requires leadership from *top management*, which is embedded across the *organization* through a robust *risk management* culture and articulated by a well-defined *risk management* policy and the associated *processes*, *roles* and accountabilities. *Top management* also establishes criteria for accepting *risk* in keeping with its organizational appetite for various types of *risk*, taking into account the *risk tolerance* of its stakeholders and the applicable regulatory environment within which the enterprise operates.

Risk management is structured and systematic, removing as much subjectivity as possible, to ensure consistent decision making. *Organizations* improve the *processes* for managing *risks* through continuous monitoring and feedback based on their experience and industry best practice.

New *risks*, affecting the *safety*, *effectiveness* and *security* of *health software* and *health IT systems*, are constantly emerging, such as *cybersecurity threats*, and require ongoing surveillance of actual and potential *risks* based on internal monitoring and industry knowledge, trends and collaboration.

5.3.2.4 Approach

As *risk management* spans the entire *product life cycle* from initial design through to *product* decommissioning, effective *risk management* includes the following:

a) proactive *risk* identification activities using ‘bottom up’ (deductive) approaches such as Failure Mode and Effect Analysis (FMEA) and ‘top down’ (inductive) approaches such as Fault Tree Analysis (FTA) and Hazard and Operability Study (HAZOPS);

b) comprehensive *risk estimation, risk analysis* and *risk evaluation* activities that consider both the potential likelihood and *severity* of harm resulting from *the hazardous situations* that are identified;

c) design, *implementation* and testing of controls to ensure *risks* are reduced to an acceptable level prior to clinical use;

c) ongoing monitoring and surveillance to detect new *risks*, emerging *threats* and the performance of implemented controls;

d) timely incident analysis, management and response that address the *root cause(s)* and are commensurate with *risks* identified post-production and during clinical use;

e) documentation of incidents, including near misses, that can be used for reporting, subsequent analysis and sharing information with other *life cycle* stage owners and peer *organizations*. ISO/TS 20405 provides guidance on *processes* and content for incident reporting.

Some *risks* cannot be managed completely by a single entity. Similar to managing *cybersecurity*, ensuring a safe *product* can require contribution and collaboration by multiple stakeholders to document and disclose *risk*-related information across the *life cycle*. Where an organization is dependent on a third-party provider of *systems*, hardware, data or IT services, the considerations are equally relevant.

5.3.2.5 Communication

Knowledge transfer through information sharing and communication is important in managing *risks* both pre- and post-*implementation*.

5.3.2.6 Information sharing at major transition points (pre-*implementation*)

Manufacturers spend significant time identifying *risks* to the patient and *user* during the design and development of their software, *systems* or devices. This informs the design, controls, and testing that are also part of their *risk management process*. After *health software*, a *health IT system* or a *medical device* is placed on the market, the *manufacturer* continues to monitor adverse *events* and malfunctions, to determine if these *risks* were identified and addressed accurately. Some of the *risks* identified cannot be fully controllable by the *manufacturer* through design mitigations and therefore should be communicated to the *customer*/*user* through comprehensive documentation, instructions for use, training materials, labelling, etc. *Assurance cases* can be used to organize and format information relevant to *risk* that needs to be incorporated throughout the *life cycle* and across several *risk* stage owners. Additional information on *assurance cases* can be found in Annex C.

The scope of information provided for connected devices should also be considered. In many cases, consideration of the "*product*-supporting infrastructure" is necessary. The *product*-supporting infrastructure is a *system* that is maintained and managed by the *manufacturer* but supports data or functionality of the device. Examples of this include analytics platforms in a cloud environment, monitoring *systems* hosted by the *manufacturer*, or a *customer*-facing dashboard with device information that helps manage non-essential information about a device such as location information. In some cases, *HDOs* can request information on this *product*-supporting infrastructure to better assess the *security* of these peripheral connected *systems*. *Manufacturers* should ensure that this type of infrastructure is secured, tested, and maintained. There should be documentation available for the management of this infrastructure. Similarly, a *manufacturer* can also receive questions from *HDOs* about the *security* and robustness of their business infrastructure that support *product* development, production and delivery.

In a similar way, there can be important knowledge to share at other transition points in the *life cycle*, such as between *system integrators*, *administrators* and *users* after the acquisition stage.

5.3.2.7 Ongoing cross-functional information sharing

For a *manufacturer* to properly monitor software, *systems* or device performance in the field, it is important that the *customer*/*user* communicates failures, near-misses, and adverse *events* to the *manufacturer* so they can determine *root causes* and track overall *risk*. In turn, the *manufacturer* should communicate and correct issues that were not expected or are occurring at a rate higher than expected.

5.3.3 *Safety* management

5.3.3.1 Statement

Safety management is the *process* for maintaining safety across the life cycle. Managing safety is an ongoing activity that involves many parties throughout the *life cycle* including organizations and the people within them. Establishing a 'culture of safety' as indicated in 5.2, coupled with organizations adopting a comprehensive set safety management practices (as outlined below), is essential for managing safety effectively. These activities include two-way communication about *health IT safety risks* and incidents within and between the parties involved.

5.3.3.2 Rationale

A common objective of *health software*, *medical devices* and *health IT systems* is to maintain *safety* and improve *effectiveness* by supporting the health and wellbeing of patients and populations, often involving sophisticated technologies, algorithms, data integration and decision support tools.

With this sophistication comes the challenge of optimizing the benefits with each *health IT implementation*, while ensuring any inadvertent negative impacts on *safety* that are introduced through the new *systems,* are appropriately managed across the *life cycle* stages by all parties involved.

5.3.3.3 Key concepts

Given the interplay between *safety* and *effectiveness*, the objective of *safety* management *processes* is to maximize the overall net benefit to patient *safety* from each *health IT system*, as well as to minimize the *risks* that a *system* can inadvertently introduce.

General features of an effective *safety* management include the following:

a) understanding the *health IT system* and how it is to be deployed and used;

b) application of *safety* management engineering principles to *health software* and *health IT systems* design;

c) awareness of how *safety* management aligns with, and leverages, other organizational *processes* such as *risk management*, patient *safety*, data *quality*, *security* and *privacy*;

d) an integrated *risk assessment process* which applies the *organization's* rigorous *risk management* methodologies and fully engages clinicians throughout;

e) *implementation* and thorough testing of the required *risk control* measures, along with documentation of any *residual risks*;

f) ongoing monitoring, education and awareness of clinical *safety risks* along with close coordination with clinical *change management* staff to optimize net clinical *safety* benefits;

g) investigation and response when *safety* incidents (including near misses) do occur. Investigation involves the use of techniques ranging from *root cause* analysis for more straightforward problems through to Systems Theoretic Accident Model and Processes (STAMP) for more complex sociotechnical problems. Response involves any resulting actions necessary to prevent re-occurrence – e.g. removing *health IT system components* from use and implementing contingency plans; notifications to affected *users*, patients or *organizations*; incident reporting and communication to regulators, *manufacturers* and *customers*; and escalation to *top management*.

Health IT safety across the *life cycle* is a shared responsibility within and between all *organizations* involved. Significant engagement in *safety* management *processes* by clinicians and IT staff is vital at all stages, with clinical leadership having an important *role* in ensuring *safety* properties are addressed and appropriate signoff's occur at key decision points.

Organizations are accountable for maintaining *safety* practices within their own sphere of activity and have a responsibility for two-way, and in some cases multi-lateral, communication about *safety risks* with upstream and downstream *organizations* involved in the *health software* and *health IT system life cycle*.

It is the responsibility of *organizations* entering into agreements to provide/acquire/operate *health software* and *health IT systems* to establish how they will communicate critical *safety* information for *risk assessment*, *risk control* and incident management.

5.3.3.4 Approach

An end-to-end approach to managing *safety* involves each *organization* adopting a culture of safety and having a comprehensive organizational *process* for identifying, documenting and managing the *safety* of *health software*, *health IT systems* and *medical devices*. Responsibilities should be clear, such as who is

responsible for ensuring that the overall benefit exceeds the *risk* of *hazards* being introduced through *health IT systems implementation* and use. This requires senior management involvement, particularly from clinicians.

Mechanisms such as *risk* registers, *safety assurance cases* and incident reporting *systems* can be used to share critical *safety* information within and across *organizations* involved in the *health software* and *health IT system life cycle* when common *processes*, formats and data elements are consistently utilized.

In a similar way to *security*, staff responsible for *safety* management require the appropriate training and organizational responsibility to oversee their *safety* management programme.

A comprehensive *safety* management programme should

a) define the *hazard* assessment, *risk control* and incident management *processes* to be used for *safety*, and how *safety* considerations are coordinated with parallel *processes* for *security* and *privacy*,

b) ensure *safety* is embedded in *health IT processes* and clinicians are engaged appropriately where *safety* considerations are involved,

c) document who is responsible in the *organization* for *safety* signoff for new *systems*, or changes to existing *systems*, prior to release,

d) define the *safety assurance case*, and/or other methods for communication between the *organizations* involved (see Annex C), and

e) ensure staff is vigilant in identifying and collaborating in response to emerging *safety* concerns.

5.3.3.5 Communication

Documentation and sharing of knowledge and information about *safety risks* is important across the *health software* and *health IT system life cycle* given the following:

a) the multiplicity of ways in which *safety risks* can be introduced at all *life cycle* stages;

b) the high levels of complexity and interdependence between *health IT systems*, *component* subsystems and data;

c) the number of parties involved across the *life cycle* stages, especially given the emergence of additional *risks* at the *implementation* and clinical use phases in particular;

d) the continuing emergence of new *risks* and the relative lack of comparable published data on the incidence and causes of *safety risks* introduced through *health IT*.

5.3.3.6 Information sharing at major transition points (pre-*implementation*)

The evaluation and documentation of *safety risks* begins at the innovation and design stage. This stage should include the involvement of IT and clinical staff who understand the range of variation in the technology, data and the clinical work environments for the target *HDOs* and *intended use(s)* of the new *system*. The sharing of information on the *safety risks* and required controls is vital for those involved in the subsequent *life cycle* stages in the *product's* development, including the acquisition and integration of software *components* from third parties into the *product*.

Once the software is ready for release to the market, documentation of the *safety risks* and controls (including *risks* that can be anticipated in the *implementation* and clinical use phases) can be communicated effectively through an *assurance case* as described in Annex C, as well as through labelling, accompanying information such as instructions for installation and use, *responsibility agreements* and other documentation. At the acquisition stage, it is important that there is good communication between the *manufacturer* and the *HDOs* about the *risks* and benefits of the *system*, as well as the alignment between the *product's intended use* and the *HDOs* planned IT and clinical operating environment. This ensures that any additional *risks* are identified and acknowledged by both parties. Post-acquisition, it is important that the documentation is updated and communicated to *customers*, as

maintenance and enhancements occur through new releases. Additionally, knowledge of *safety risks* and mitigations is gained through the analysis of incident reports as well as new intelligence about *safety risks* from published research and healthcare industry learnings.

As described in Clause 4, *health software* and *systems* are implemented by *HDO's* into a complex and multi-faceted sociotechnical ecosystem, where several different parties (including contracted resources) and different disciplines (IT, clinical information management, etc.) can be involved. Comprehensive and clearly written communication is vital at all stages across the *life cycle*. The responsible *organization* should be confident that the *safety* aspects of introducing a new *health IT system* have been appropriately understood and managed prior to signoff for 'go live'.

5.3.3.7 Ongoing cross-functional information sharing

Complex *health IT implementations* are often implemented in stages so that the impact of the new *system* on an *HDO's* infrastructure, clinical work environment, together with unanticipated impacts on other areas of the sociotechnical *system*, can be managed. Information and knowledge sharing in the early post-*implementation* stages is an important catalyst in maturing the *implementation* and clinical adoption of the *system* to maximize its *effectiveness*.

At the operational and use phase, *health IT systems* continue to evolve, and two-way cross-function communication is vital in this dynamic ecosystem. This evolution occurs at the *manufacturer's* level with *product* maintenance and enhancements as well as at the *HDO's* operational level with changes in local infrastructure, integration points with other *systems*, data sources and uses for the new *system*.

Since knowledge of *safety* issues related to *health software* and *health IT systems* continues to evolve and grow, transparency in sharing of data on incidents is important within and between *organizations*. ISO/TS 20405 provides a framework to facilitate communication of *safety* incident data in a way that supports effective sharing between parties in managing incidents. ISO/TS 20405 also supports the aggregation of incidents across the healthcare industry to support surveillance and facilitate knowledge development and sharing in order to identify and better manage emerging *risks*.

5.3.4 *Security* management

5.3.4.1 Statement

Security management is the *process* of maintaining *security* across the *life cycle.* The *security* of *product*, *system*, or network is interdependent on the surrounding layers of *products*, *systems*, and networks. *Security* management considers all aspects from physical *security* of the actual hardware *components* to the *security* of the data stored on the technologies.

5.3.4.2 Rationale

With the digitization of healthcare, *security* is becoming increasingly important. It enables software, *medical devices*, *systems* and other *health IT assets,* including data and information, to operate as intended, delivering safe and effective patient care. Connected *systems* create environments where *security events* can escalate quickly, so prevention is crucial to *security*.

Maintaining appropriate cyber hygiene is also a critical vehicle for maintaining *privacy*.

5.3.4.3 Key concepts

Security involves the protection of three main elements:

a) Confidentiality: the protection of information from the disclosure to unauthorized parties;

b) Integrity: the protection of information from being modified by unauthorized *users*;

c) Availability: the assurance that authorized parties are able to access the information when needed.

From a systems perspective, integrity is the protection of a system's capability to perform according to its intended function without being degraded or impaired by changes or disruptions, and availability ensures that infrastructure resources are available to maintain operation under normal circumstances in order to serve its intended purpose.

These three main elements should also be protected from impacts that are not caused by unauthorized activities, such as use errors or electromagnetic interference. Such occurrences are beyond security management but should be covered by risk management in general.

Security management involves ongoing monitoring and *vulnerability* management. New vulnerabilities emerge through internal errors (for example, coding and configuration errors) and through adversarial attacks. It is important for *security risk* owners at each stage to have *processes* in place to identify new vulnerabilities, including monitoring sources of industry-specific *threats*. This enables a proactive treatment of *security risks*.

To allow for forensics analysis of *events* and *root cause* analysis, it is important to include audit logging functionality in *systems* and networks.

Security events can evolve quickly and spread across a *system* once certain external *security* layers such as a firewall, are breached. Therefore, it is important to have established and practised incident response plans.

Effective hardening occurs in layers, at each health IT *component*, at each *system*, and through the network and infrastructure. Otherwise, once one layer is breached, the entire network can be impacted quickly. Layers of *security* also help to prevent escalation activities by an active attack.

Effective *security* management is essential to ensuring effective *privacy* management. *Security* controls are critical for data protection and *privacy,* and therefore it is essential that these are developed and maintained in a coordinated manner. Effective *security* management is also important to human factors; however, the relationship is reversed. Certain *security* controls can have an adverse impact on the *usability* of a *product* or *system*. Therefore, stage *security risk* owners should consider the impact to *usability* when establishing controls. This relationship should not be considered a trade-off. Instead, each *security* control decision should consider impacts to *usability* so that the best design control option is selected.

Security controls that do not take clinical workflow and human factors into account have a higher chance of being disabled or otherwise circumvented. Well-designed *security* controls are robust and integrate as seamlessly as possible into the workflow, to avoid adverse impacts on patient care.

5.3.4.4 Approach

Security management is a shared responsibility requiring ongoing monitoring as new *threat* and vulnerabilities evolve. These types of *risks* require careful coordination between stakeholders, with quick response, communication, and remediation, depending on the type of *threat*.

For *manufacturers* and *developers*, establishing *cybersecurity* for a *medical device*, *health software*, or *health IT system* is not merely adding functional *security* requirements to a *system*. It requires appropriate *security* management during the entire *product life cycle.* Such management can only be achieved by establishing the necessary *processes* and standards to be applied and executed by the *manufacturer* and other stakeholders. Each *organization* should establish *processes* and objectives for *security* management such as *security* requirements collection, *security* by design objectives, *security risk management*, supplier management, secure *implementation* and operation, and *security verification* and validation. It also includes management of *security*-related issues including *threat* landscape monitoring and incident handling, *security* update management and the creation of *security* guidelines. This requires the creation and maintenance of a controlled *security risk management file* for each *product*.

Healthcare delivery organizations establish *security* requirements for their *systems* and collect *security* information from *manufacturers* and vendors to better understand the types of *risks* in the context of their *health IT infrastructure*. Ongoing monitoring for new *threats* is often carried out by both

manufacturers and *HDOs* to allow for rapid identification and coordinated control of emerging *threats* throughout the *life cycle*.

Guidance on *product security* requirements using a high-level set of *security capabilities* is available in publications such as IEC/TR 80001-2-2. This Technical Report highlights *security* and *privacy* features such as: Automatic Logoff, Audit Controls, Authorization, Configuration of *Security* Features, *Cybersecurity Product* Upgrades, Personal Data De-Identification, Data Backup and Disaster Recovery, Emergency Access, Personal Data Integrity and Authenticity. Malware Detection / Protection, Node Authentication, Person Authentication, Physical Locks on Devices, *System* and OS Hardening, Service Access *Security*, *Security* and *Privacy* Guidance, Personal Data Storage Confidentiality, Transmission Confidentiality and Transmission Integrity.

Further guidance for the establishment of each of the security capabilities presented in IEC/TR 80001-2-2 is documented in IEC/TR 80001-2-8. ISO 27799 also provides useful guidelines for organizational information *security* standards and information *security* management practices including the selection, *implementation* and management of controls taking into consideration the healthcare *organization's* information *security risk* environment(s).

5.3.4.5 Communication

Communication amongst stakeholders and industry is essential to share awareness and alert others to potential *threats*. This enables a proactive approach to *security* and to awareness of potential active *exploits*. Strong *security* management is a collaboration between *security risk* owners at each stage of the *life cycle*, to establish layers of protection and coordination of *security* controls across the *life cycle*. This includes having a secure environment at all stages of the *life cycle* (for example, in developing, manufacturing, implementing and operating *health IT systems*) and using mechanisms such as *security assurance cases* to document and communicate information.

5.3.4.6 Information sharing at major transition points (pre-*implementation*)

During the transition between vendor and *customer*/*user*, there is a significant amount of information that should be shared to ensure that the subsequent *life cycle* stage *security* owners have the information to enable continued oversight of *security* for the new software, *system* or device as well as the *user's* overall network. This information can include a *manufacturer's* disclosure statement, for example the *Manufacturer's* Disclosure Statement for *Medical Device Security* (MDS2), configuration requirements, architectural diagrams of the *system*, *vulnerability* assessments, *and health software component* information (i.e. software bill of materials – sBOM). This information is needed for the *life cycle* stage *security* owner to accurately assess the incoming software, *system* or device and to ensure secure integration and *implementation*. *Process* information can also be expected by specific *HDOs*, including *vulnerability* monitoring methodology, *vulnerability* disclosure practices, and patch management expectations.

Information sharing is an important element of the shared responsibility between each stakeholder for managing security within a healthcare environment. Each stakeholder has a key role to play to ensure that *health software* and their third-party software *components* are kept patched. However, communication is crucial to identify impacted systems and coordinate the actions necessary to maintain their security controls. Communication is also critical for helping to identify potential incident and trace impacts.

5.3.4.7 Ongoing cross-functional information sharing

Security management presents some unique cross-functional information sharing expectations. Since vulnerabilities are constantly emerging, both *manufacturers* and *HDOs* should constantly monitor for new *threats* to their *systems*. Ongoing *vulnerability* monitoring is necessary and new vulnerabilities can require immediate communication to the *HDO*/*user* to ensure that proactive action can be taken to prevent exploitation and potential patient *harm*. In some cases, vulnerabilities will require a patch to fully address the issue. However, these patches require some level of validation and therefore it is important that the *manufacturer* and *HDO* have communication channels in place to coordinate the management of new vulnerabilities.

In other circumstances, the *HDO* can discover a new *vulnerability* through scanning or a device that becomes infected with malicious code. This is another opportunity to leverage existing communication channels so that the *HDO* can notify the *manufacturer* and ensure a timely response. The *manufacturer* will then assess the potential impact to other devices and can initiate an incident response *process*.

During a global *cybersecurity event*, cross-functional communication is vital. Malware that is designed to attack a common software *component* such as an operating *system* can travel quickly and affect many *systems* and networks within hours or days. Both *HDOs* and *manufacturers* should have incident response plans that consider these types of attacks and establish communication channels that can support a large-scale, global *event*. Incident response plans should be scalable to large numbers of affected devices, inclusive of all necessary stakeholders.

5.3.5 *Privacy* management

5.3.5.1 Statement

Privacy management is the *process* of protecting the *personal health information* of individuals against privacy breaches.

5.3.5.2 Rationale

Privacy is a critical element for safe and effective healthcare delivery because

a) patients can be *harmed* physically or emotionally if their *privacy* is compromised (i.e. unauthorized disclosures are a *risk* that can be protected against through *security* and other measures), and

b) the benefits (*effectiveness*) of *health IT systems* are compromised when the willingness of patients and care providers to share sensitive health information relies on their trust that *privacy* requirements will be met.

5.3.5.3 Key concepts and principles

For *health software* and *health IT systems*, *privacy* is concerned with *personal health information* relating to the physical and mental health of the individual. In the provision of health services to the individual this can include the following types of information as identified in ISO 27799:2016:

— information about the registration of the individual for the provision of health services;

— information about payments or eligibility for healthcare in respect to the individual;

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

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

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

— identification of a person (for example a health professional) as provider of healthcare to the individual.

Privacy protection begins with understanding the purposes and rights (limitations) regarding the collection of *personal health information*, including both primary and secondary uses of information

Jurisdictional laws and regulations, professional ethics and organizational policies for *privacy* play a vital *role* in defining the rights of individuals to *privacy* in relation to their health care information by establishing the following:

a) how patient consent for use and disclosures can be obtained and the degree to which consent is explicit, implied or deemed in specific circumstances;

b) limits and conditions on the uses and disclosures that can be made of such information with and without patient authorization;

c) patient rights to access their records and request corrections;

d) when and how patients are advised where *privacy* breaches occur.

Patient consent for *privacy* purposes is more meaningful when it is informed consent — whether the consent is explicit, implied or deemed.

Privacy and *security* go hand-in-hand, and *privacy* should also be monitored as new *threats* and vulnerabilities emerge constantly, with good bi-directional communication between stage owners across the *systems life cycle*.

Training and awareness amongst patients and health providers about *privacy* protection can be as important as physical safeguards.

Privacy risks are assessed and controlled in a way that appropriately balances the need for explicit consent and strict controls based on the *harm* that can be caused to individuals if a *privacy* breach occurs. In addition, consideration of the potentially negative impact of tight *privacy* controls on health care service delivery and *effectiveness* should be given – for example where delays in care provision occur when important information is not available in critical care situations.

5.3.5.4 Approach

In a similar manner as *safety* and *security*, a comprehensive approach to *privacy* is required across the *systems life cycle*. Some of the major elements in a *privacy* strategy include the following:

a) Privacy by design – a proactive approach to avoiding the 'layering on' of *privacy* controls by embedding *privacy* considerations into the design of new *systems* including

   — features such as *system* defaults and *user* open and transparent documentation supporting the selection and *verification* of *privacy* controls by downstream parties such as *system integrators* and *HDO's*, and

   — leveraging software and *system security* features across the *life cycle*.

b) Privacy impact assessment (PIA) – in a similar way as *security threat-risk assessments*, PIA's are used by *organizations* to assess and document the *risks* (and associated impacts) to *privacy* that could occur with a *system implementation* and to evaluate *risk control* options. The PIA typically also serves an important *role* for *organizations* in ensuring conformance with *privacy* policies as well as regulatory and legal requirements.

c) Organizational privacy policies and ongoing education – *privacy* is often impacted by human action and healthcare often involves handling and communicating very sensitive information. A comprehensive set of *privacy* policies (backed by an ongoing education programme) is very important so that staff, patients and families understand how to handle the wide variety of situations involving the collection and disclosure of *personal health information*. Consideration should be given to establishing a Privacy Information Management System (PIMS) for privacy management within the context of the organization as detailed in ISO/IEC 27701.

5.3.5.5 Communication

It is important that stakeholders working with connected devices and *health IT systems* share information about *hazards*, controls and *risks* associated with the *implementation*, operation and use so that *privacy risks* can be minimized, and the integrity of controls maximized. This also becomes important when providing or following guidelines for proper disposal of *health IT systems* and devices that contain personally identifiable information.

5.3.5.6 Information sharing at major transition points (pre-*implementation*)

Consideration of *privacy* requirements begins at the innovation and design stage (*manufacturers*) and the acquisition stage (*HDOs*). Formalized *privacy* impact assessments are a commonly used tool to define and document *privacy* requirements, identify *risks*, specify the necessary controls and assess their *effectiveness* in meeting organizational and regulatory requirements regarding *privacy*. These assessments can be an effective tool for communicating information between *roles* and *organizations* across the *life cycle*, beginning with the communication between *manufacturers* and *HDOs* at the point new *health software* or *health IT systems* are being acquired or developed. This communication should continue through the subsequent stages where *integrators* and other third parties are involved.

5.3.5.7 Ongoing cross-functional information sharing

Where *privacy* breaches occur, requirements defining what information needs to be communicated about the breach, as well as to whom and when, are typically defined by jurisdictional *privacy* regulations. In addition, communication of personally non-identifiable information can be necessary for assessing and addressing the underlying causes of *privacy* incidents and preventing their re-occurrence. It is important to communicate this information between *roles* in a similar way to *security* and *safety* incident information. *HDOs* should also review and update their *privacy* impact assessments at regular intervals, and this is a good opportunity for collaboration between *roles*.

Annex A
(informative)

Rationale

A.1 General

This annex provides a rationale for terms and concepts related to this document. It is intended for those who are familiar with the subject of this document but who did not participate in its development.

A.2 Rationale

Clause 3 - Terms and definitions

The goal for this document is to identify the best common definition for use across the *life cycle*. As a result, some of the terms defined in this document are not used extensively in this document but do contribute to the larger goal of establishing this common language across the *life cycle*.

International standards focusing on connected health *products* and *health software* have been considered. The ISO 80001 and the IEC 80001 series and IEC 62304 were specifically considered for the scope of terminology selected with the goal of providing a foundational set of terminology for *health software*. ISO 14971, ISO 13485, ISO 9000 family, ISO 31000 and several ISO and IEC Guides were referenced and leveraged when selecting terminology and aligning *process* with industry norms.

The identification of a common definition for every term is not possible due to actual contextual differences in the application of these terms at different points in the *life cycle*. One example of this is the term "risk" (see 3.4.10)."

However, risk is defined, as seen in ISO 31000:2018, 3.1, to include both positive and negative risk. This is commonly practised in more business-specific applications (as in ISO 31000). While there is certainly value in approaching *risk management* this way, for the purposes of maintaining the *key properties* of *safety*, *effectiveness*, and *security*, the definition from ISO Guide 63 has been selected as the most appropriate context. This does not prevent the users of this document from broadening the way in which they handle the effects of uncertainty, but it does ensure that the way risk is used in this document is consistent and well-understood.

***Usability* (3.2.15) and human factors**

Human factors and *usability* involve a discipline with a goal to improve the interface for human use. Human factors engineering and *usability* engineering are considered equivalent in IEC 62366-1:2015. However, the concepts are sometimes differentiated. In this document, the terms are used interchangeably. However, the application of human factors and *usability* engineering differs across the *life cycle*. For example, for *medical device manufacturers* the application of IEC 62366-1 is foundational for designing *medical devices* that create a positive and effective *user* experience, sometimes called *user*-centered design. From the *HDO* perspective, the application of human factors and *usability* needs to put a greater focus on the *process* and clinical workflow aspects of their practice. However, it is important that all stakeholders understand how this discipline can vary across the stages in the *life cycle* to ensure clear communication of *risks* and controls.

***Health IT infrastructure* (3.3.7), health *IT networks* (3.3.11) and medical IT-networks**

A connected *healthcare delivery organization* faces the challenge of complicated *systems*, interconnected networks, and interdependencies within their information technology management. Even assigning a commonly-understood or commonly used name for the various parts is challenging. As such, several terms have been defined as part of the goal to provide a common language when describing these

systems and networks. IEC 80001-1 used the term "medical *IT-network*" to describe the network that hosted and supported the *medical device(s)* within the hospital. In the search for a term that can apply to the broader scope of *medical devices*, *health software*, and other supporting infrastructure, this document uses the term "*health IT infrastructure*" to identify the infrastructure that not only supports but includes *health software*. The health IT infrastructure can include one of more medical devices, software as a medical device (SaMD), health IT systems, as well as other IT infrastructure *components* and cloud-based solutions. It is important to identify and manage this infrastructure for the purposes of maintaining the *safety*, *effectiveness*, and *security* of its *components* and the connected *health software*, *medical devices* and *health IT systems* that leverage them. Figure 2 provides a visual representation of these *components* and their interrelationships.

Health software (3.3.9) and Software as a Medical Device

Health software is a term that has emerged, which refers to software that is used to manage, maintain, or improve health or delivery of care. Since regional jurisdictions have differing regulations concerning which software is considered a *medical device* (and these regulations can evolve over time), this document is agnostic concerning whether or not *health software* is regulated. Whether regulated or not, the *quality* and *effectiveness* of how *health software* is developed and maintained is important. Therefore, International Standards such as IEC 62304 have altered their scope in recent revisions to include *health software* rather than restricting it to *medical device* software. In a related International Standard, IEC 82304-1, the focus is shifted slightly to focus only on software that is placed on the market without dedicated hardware. Both International Standards use the term "*health software*" but their scopes are different. This document uses the more general definition of *health software* and includes both embedded software *products* and software-only *products*.

Software as a *Medical Device* (SaMD) is a term that has evolved to better describe *medical devices* that are comprised solely of software. The International Medical Device Regulators Forum (IMDRF) has defined this term to refer to "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware *medical device*"[14]. In the past, this type of software had been referred to as "standalone software" but this created confusion for some because it was occasionally interpreted as software that did not connect to other *systems*, which was not how this term is intended to be used. Therefore, this new term, SaMD, was developed and put into use. Some regulators, including the US FDA, have put these terms into use in their regional regulations and guidance. SaMD is distinguished from *health software*: *health software* can include software that is not a *medical device* as well as software that is embedded in a physical device.

An additional term, Software in a *Medical device* or SiMD, has been introduced but is currently less commonly used than SaMD. SiMD is defined as "software intended to be used for one or more medical purposes that perform these purposes as part of a hardware *medical device*" and is often called "embedded software." However, for the sake of transparency and understanding alternate terminology, it is included here as supplementary information.

***Security* (3.2.13), *cybersecurity*, information security, data and system security, and *vulnerability* (3.4.22)**

To align with industry norms, this document diverts from the use of "data and *system security*" as used previously in the IEC 80001 series and others, and simplifies this by defining, and using, the basic term "*security*" to refer to the *process* of safeguarding *assets* in both physical and digital format. Technically, *cybersecurity* can be considered a subset of *security*. *Cybersecurity* deals with protecting data and information that is in digital or electronic form. However, in actual usage, *security* and *cybersecurity* are often interchanged. This is the case in certain regional *medical device* regulatory guidance on the issue as well. Therefore, after careful consideration, this document does not seek to define these terms separately. *Cybersecurity* is listed as an admitted term to *security*. This decision was made because it was felt that although defining them separately could be technically correct, it would likely lead to confusion for the reader since the terms are so often interchanged in common usage.

Information *security* is commonly defined in the traditional IT *security* context, but it is not leveraged in this document. In general, *security* is used to describe most *processes* and activities that are addressed as part of the *life cycle* of connected healthcare IT *assets*.

The definition of security is risk-based. This considers that an absolute protection from unauthorized activities cannot be achieved in practice while maintaining the necessary level of effectiveness.

This risk concept is well known and proven for other types of adverse effects on medical devices and health IT systems, for example, ISO 14971.

The definition addresses two aspects related to this specific type of risk: Unauthorized activities as sources (or adverse events) and confidentiality, integrity and availability that need to be protected from these activities in order to be maintained at acceptable level. However, the protection of confidentiality, integrity and availability is not specific for security as it can also be compromised by other adverse effects like use errors or electromagnetic radiation. Furthermore, the evaluation whether the risk related to confidentiality, integrity and availability is acceptable may need to consider the intended use of the health IT system. When considering the intended use, the severity of the potential harm to people or the organization and the likelihood of that harm can be determined and used for evaluation whether the risk is acceptable. This allows, as an option, for defining acceptance criteria that are consistent with those for other risks resulting in the same harm. Another option is to define acceptance criteria in conjunction with the application of dedicated security risk scoring methodology (such as CVSS). Regardless, it is important to consider intended use and environment of use when defining acceptance criteria.

Suppliers of components of a health IT System might not be aware of the complete intended use of the health IT system and therefore their risk evaluation might be limited to consider only the effects on confidentiality, integrity and availability at the interfaces of their products. Remark: That is again not specific for security but applies to safety in general.

Vulnerabilities, as used in security, are used in a specific context of a security weakness and not in the more general sense.

***Risk management* (3.4.16) and probability**

Manufacturers and developers utilizing an ISO 31000 risk management process should be aware of the different vocabulary and concepts used between ISO 31000 and ISO 14971. This document is focused on areas necessary to ensure the safety, effectiveness, and both data and system security (including privacy) of health software and health IT systems. For the purposes of this document, the vocabulary and concepts of ISO 14971 are used to support this focus. The rationale for this subclause explains how one can translate these vocabulary and concepts.

ISO 31000 is a generic risk management International Standard and any references to safety are informative. That International Standard does not deal specifically with safety. ISO 14971 is a safety-related risk management International Standard. Because of these differences in focus, the two International Standards use different terms for similar concepts and different definitions for the same term. Table A.1 compares these terms and concepts.

Table A.1 — Relationship between ISO 31000 and ISO 14971 terms and concepts

ISO 31000 term	ISO 31000 definition	ISO 14971 term	ISO 14971 definition	Relationship
risk management	coordinated activities to direct and control an *organization* with regard to risk (ISO 31000)	*risk management*	systematic application of management policies, procedures and practices to the tasks of analysing, evaluating, controlling and monitoring *risk* (ISO 14971)	aspect of risk management (ISO 31000) related to the systematic application of management policies, procedures and practices to the tasks of analysing, evaluating, controlling and monitoring *risk* (ISO 14971)

Table A.1 *(continued)*

ISO 31000 term	ISO 31000 definition	ISO 14971 term	ISO 14971 definition	Relationship
risk	effect of uncertainty on objectives	*risk*	combination of the probability of occurrence of *harm* and the *severity* of that *harm*	aspect of risk (ISO 31000) related to the combination of the probability of occurrence of *harm* and the *severity* of that *harm* NOTE this is also related to the approach taken in IEC 62304 for determining safety classification where the probability of a software failure is considered 1.
consequence	outcome of an event affecting objectives where event means: occurrence or change of a particular set of circumstances	*harm*	injury or damage to the health of people, or damage to property or the environment	consequence (ISO 31000) that can cause injury or damage to the health of people, or damage to property or the environment
risk source	element which alone or in combination has the intrinsic potential to give rise to risk (ISO 31000)	*hazardous situation*	circumstance in which people, property or the environment is/are exposed to one or more *hazards*	risk source (ISO 31000) in which people, property or the environment are exposed to one or more *hazards*
likelihood	chance of something happening	probability	Not defined	The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. For the purpose of *health software*, probability should be interpreted to mean the chance of something happening and not interpreted as a mathematical term.

Annex B
(informative)

Concept diagrams

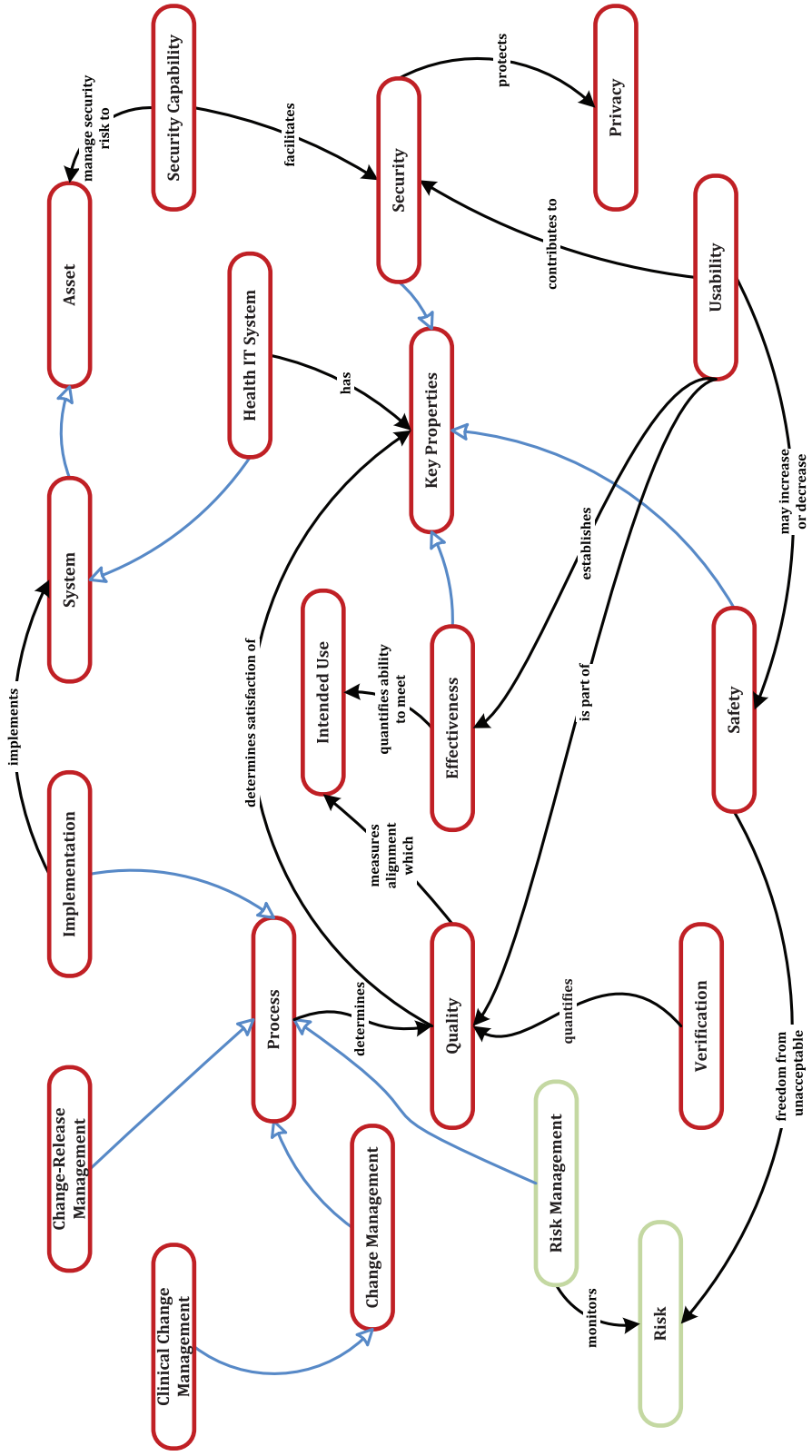
B.1 Overview of concept diagrams

The concept diagrams B.2 present diagrammatic representation for systems of concepts used in this document. The diagrams take the terms and definitions and group these into generic concepts that can assist in understanding the context of use of the terms and the relationship between terms. Each concept diagram represents one aspect of a related group of terms and the interaction between these terms within their context of use.

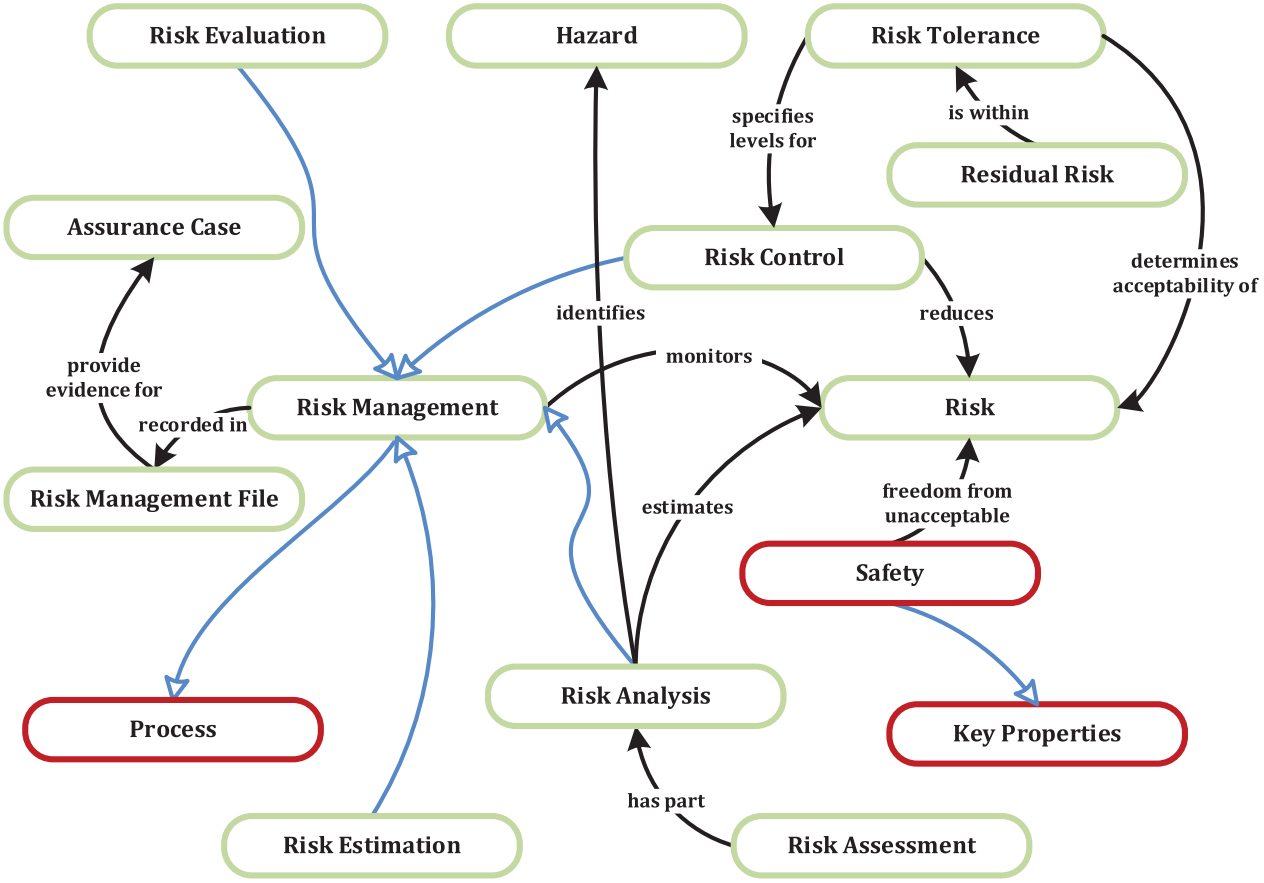
The concept diagrams in Figure B.1, are designed to improve understanding and the use of the terms, by creating a common understanding in the use of these terms with regard to this document and other associated standard such as the ISO 80001 and the IEC 80001 series.

The concept diagrams describe the association between terms and the nature of this association, and adopt the approach defined in ISO 13940:2015 *Health informatics — System of concepts to support continuity of care*. The diagrams refer to the conceptual level only and do not include details of *implementation*.

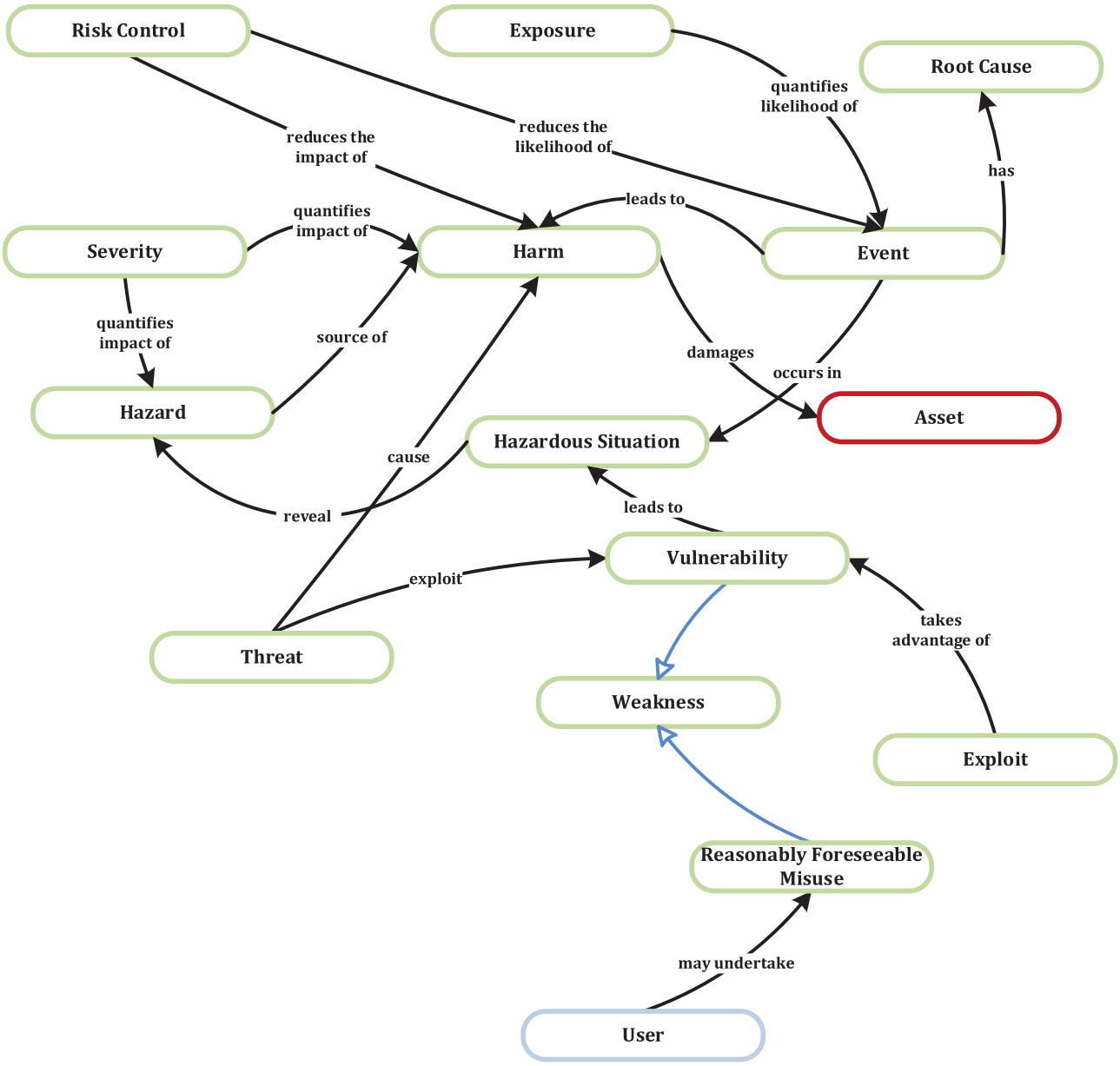
B.2 Concept diagrams



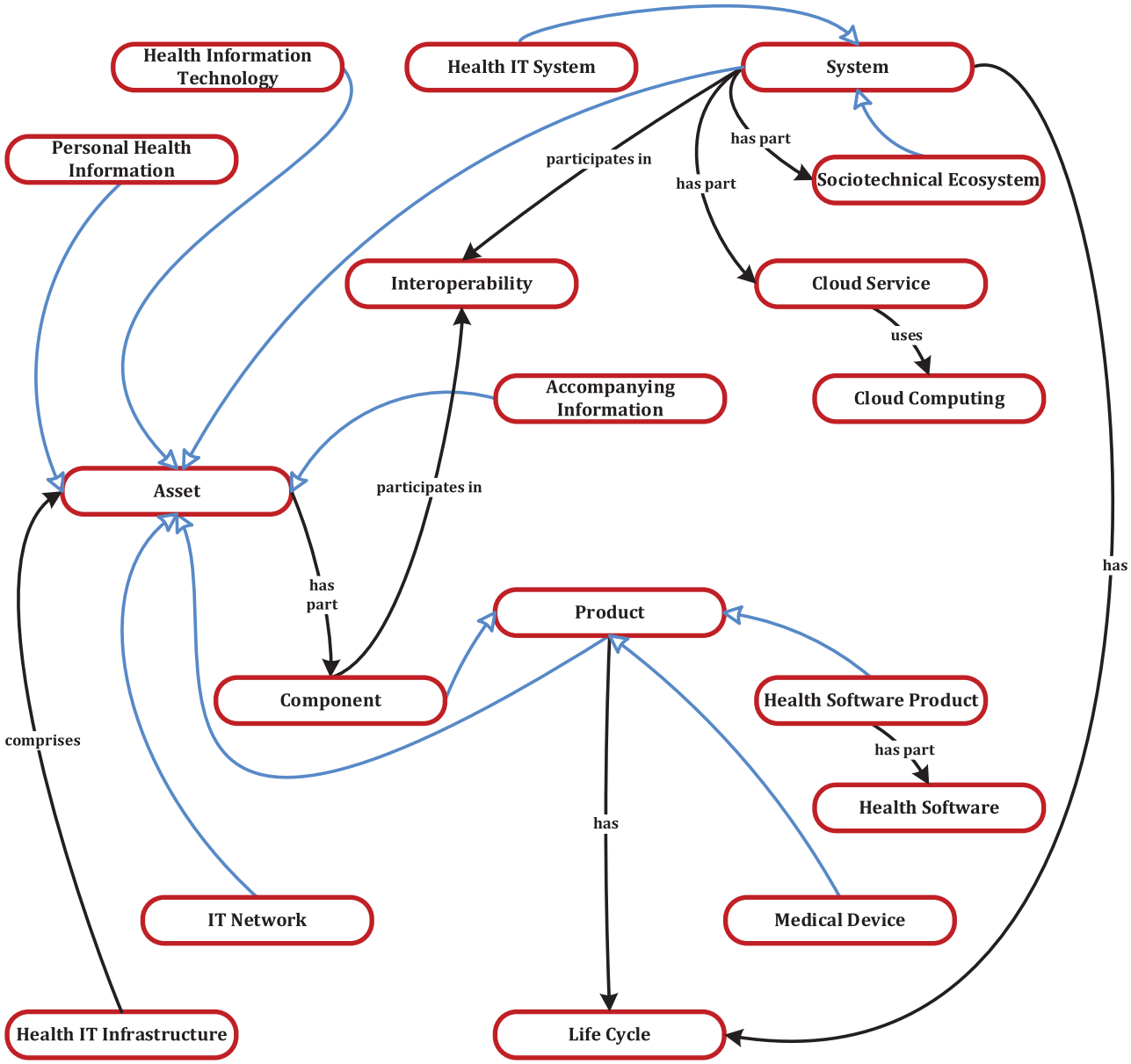
a) Relationship between Key Properties and Processes



b) Relationship between Risk Management concepts



c) Relationship between Harm concepts



d) Relationship between Health Information and Technology concepts

Key

relationship

is a kind of

Figure B.1 — Concept diagrams

Annex C
(informative)

Use of *assurance cases* for knowledge transfer

C.1 Overview

The *assurance case* is a structured argument which is supported by a body of relevant evidence that provides a compelling, comprehensible and valid case that a *health IT system* can be used safely and securely. The structured argument provides an explanation of how the supporting evidence demonstrates that the *health IT system* exhibits an adequate degree of *safety* and *security*, which demonstrates compliance with requirements and sufficient *risk control* measures for identified *hazards*. The supporting evidence can be the result of observation, analysis, testing or simulation that provides information that an integrated *health IT system* is safe for use.

The *assurance case* is more than a physical set of documents, as it encompasses the intellectual planning for establishing the argument and generating the supporting evidence. Establishing the argument as soon as practical in the *life cycle* ensures that resource and effort is directed efficiently to generate relevant evidence. If consideration of the *safety* and *security* arguments are left until later in the *life cycle* it can become difficult to explain how the available evidence supports claims of the *key properties* of the *health IT system*. Such an approach can result in gaps or lack of evidence which can result in additional work, delays and increased costs.

The *assurance case* will evolve during the *life cycle* of the *health IT system* and shall be reviewed to ensure that it continues to provide sufficient confidence in the *key properties* of the *health IT system*.

The *assurance case* report is the physical document that summarises all the key elements of the *assurance case* and references all supporting material in a clear, comprehensible and concise format. It serves to communicate the *assurance case* to the end *users* and *top management* and is also an important vehicle for the communication and transfer of *risk*-related information between *roles* across the *health IT system life cycle* as discussed in 4.6.

The relationship between the *risk management file*, the *assurance case* and the *assurance case* report can be understood by considering a filing cabinet.

1) The **filing cabinet** can be thought of as the *risk management file*, i.e. the repository in which relevant information is stored.

2) The **organization, indexing and cross referencing** of the information within the filing cabinet can be thought of as the *assurance case*, i.e. the planning and structure.

3) The **retrieval and presentation of information** from the filing cabinet at any point in the *life cycle* can be thought of as the *assurance case* **report**.

Assurance cases can be an extremely useful tool for managing *risk* across the *life cycle* of *health IT systems*. *Manufacturers* can utilize an *assurance case* to manage and communicate the *risks* associated with their *products* within their companies and as those *products* are transferred to the *customer*. An *HDO* can then build upon the information the *manufacturer* has provided and develop its *assurance case* as the *product* is integrated, configured, and implemented for use within their particular sociotechnical ecosystem context. In this way, *assurance cases* provide a continuous thread for all *roles* involved during the *life cycle* in managing the collective *risks* of all the *components* across the *health IT infrastructure*, including the *health software*, *medical devices* and other *health IT systems* that make up these complex *sociotechnical ecosystems*. Additionally, *assurance case* reports can be generated for the purpose of communicating *risks* from one stakeholder to another as ownership of a *health IT system* changes hands.

There are three key parts that make up an *assurance case*:

– a structured **argument**;

– a body of **evidence**;

– a compelling and comprehensible **claim**.

Each of these elements should be developed by following the guidelines provided in C.3.

An *assurance case* can be built in a variety of notation styles. These include textual, tabular, and graphical. *Assurance cases* for large complex *systems* can include several or all of these styles. Overall, however, it is most important that the representation is clear, comprehensible to all stakeholders, and can be reviewed and maintained effectively.

C.2 Structuring the *assurance case* claim and argument

The claims created in an *assurance case* are often tiered into a top claim of *safety* and *security*, followed by a set of sub-claims.

An example top claim is "ACME software is adequately safe and secure for its *intended use*."

Example sub-claims include the following:

— The *safety risks* associated with ACME software are reduced to an acceptable level.

— The *security risks* associated with ACME software are reduced to an acceptable level.

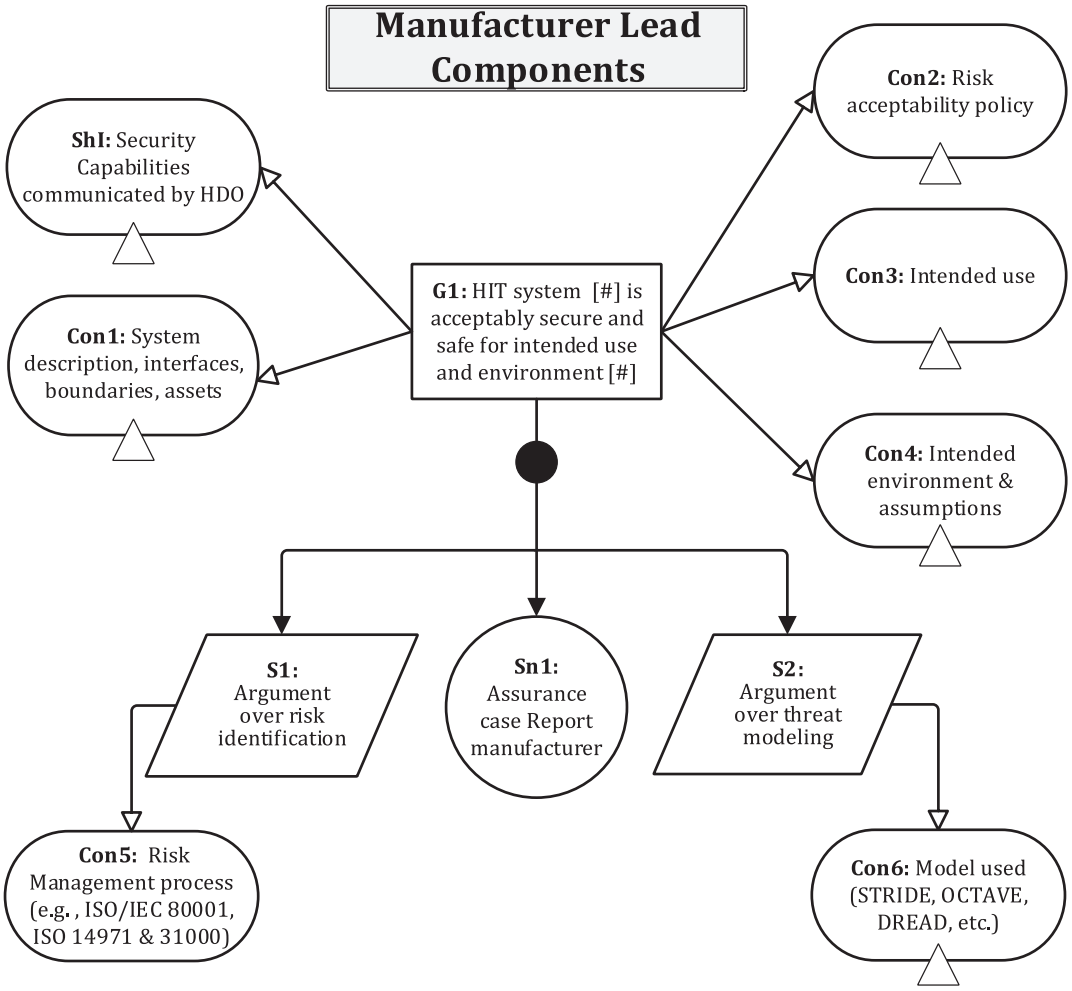
The following examples express the *assurance case* argument established from the perspective of

a) a *manufacturer* (Figure C.1 to Figure C.3), and

b) a *healthcare delivery organization* (Figure C.4 and Figure C.5).

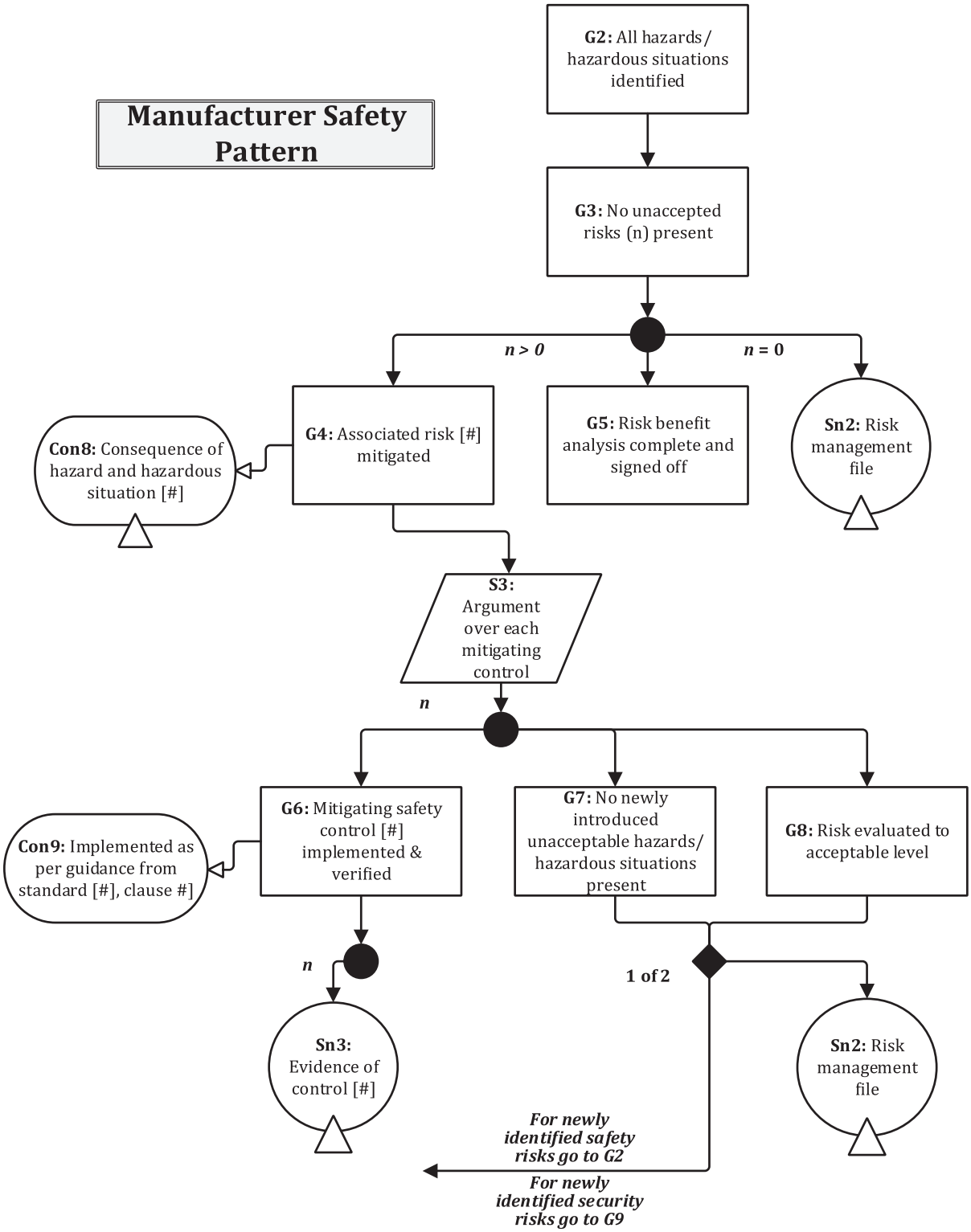
These examples (Figure C.1 to Figure C.5) illustrate the typical patterns for an *assurance case* for a *health IT system* and are in the form of Goal Structured Notation (GSN) [48].

a) **Manufacturing *organization* patterns**



GSN Construct	Description
G1	High level claim regarding acceptable *safety* and *security* characteristics of the *health IT system* when used as intended in the intended environment
CON1...CON4	Contextual information that supports G1 (and subsequent goals). Effectively defines the environment in which the *assurance case* holds. E.g. CON2 establishes the *organization's* position on *risk* acceptability.
SH1	*Security* capabilities that have been established by the *HDO*
S1, Sn1, S2	The "and" combination of argument elements through which G1 is substantiated. S1 and S2 are strategies that establish how *safety* and *security* characteristics will be assured through the claims G2 and G9 in figures C.2 & C.3 respectively. Sn1 is a solution, in this case the *assurance case* report which summarises the assurance achievement and when communicated to the *HDO* provides important contextual input (see CON4 in Figure C.4).
CON5, CON6	Contextual information that has an influence on the related strategies e.g. CON5 provides the framework on which *risk management* is conducted.

Figure C.1 — *Manufacturer* top level lead *components*

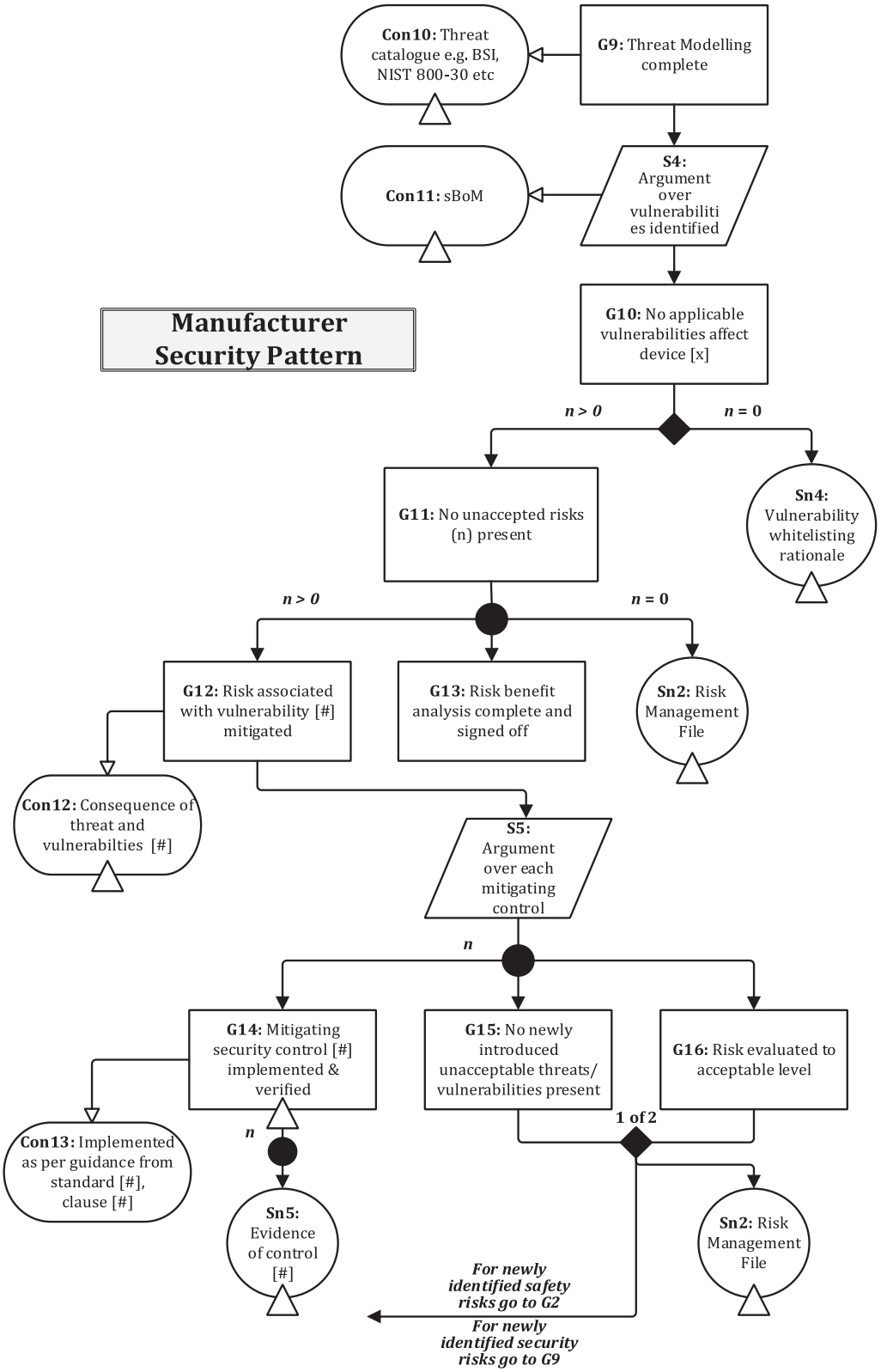


GSN Construct	Description
G2, G3	Claim based on *effectiveness* of *hazard risk management* in identifying all foreseeable *hazards* and managing associated *risks* to a level where they are accepted by the *organization*.
G4, G5, Sn2	The "or" combination of argument elements through which G3 is substantiated. Where *hazards* are identified G4 establishes that the related *risk* has been mitigated. If this claim cannot be substantiated, then G5 establishes that a benefit-*risk analysis* has been undertaken and the *risk* is accepted by the *organization*. Sn2 applies where no *hazards* are identified.

GSN Construct	Description
S3	Establishes the strategy through which G4 is substantiated i.e. for each *hazard*: • mitigating *risk controls* are implemented and verified (G6) and • no new unaccepted *hazards* are introduced as a consequence of G6 (G7) and • the *hazard risk* has been evaluated as being acceptable (G8).
G7, G8	If these goals cannot be substantiated, a need for further work is required. From a *safety* perspective, further assurance from G2 needs to be provided. From a *security* perspective, further assurance from G9 (Figure C.3) needs to be provided. Where the goals can be substantiated this is recorded in the *risk management file* (Sn2).
Sn3	Evidence of effective *risk control* measures in substantiation of G6.
CON9	Contextual information that influences the *risk control* measure *implementation* e.g. relative strengths of different *risk control* types.

Figure C.2 — *Manufacturer safety* pattern

In Figure C.1, both the *safety* and *security* patterns flow from the top-level claim. The *security* pattern in Figure C.3 is similar in structure to that in Figure C.2 but focuses on *threats* and vulnerabilities related to *security risks*. At the bottom of Figure C.2 and Figure C.3, any newly identified *safety* and *security risks* then loop back to G2 (for *safety risks*) or G9 (for *security risks*). This illustrates the iterative nature of the *process* as well as the interdependence between *safety* and *security risks*.



GSN Construct	Description
G9	Establishes that *security risk management* is initiated by undertaking and completing *threat* modelling.
CON10, CON11	Establishes the *threat* catalogue to use in the modelling (G9) and the *assets* to which it is applied.
S4	Establishes the strategy through which G9 is substantiated i.e. management of vulnerabilities that are identified by the *threat* modelling.
G10 onwards	Essentially mirrors the *safety* goal G2 but in the context of the *risk* of *security* vulnerabilities.

GSN Construct	Description
Sn4	Generic vulnerabilities that can have been identified for a specific *component* but are not applicable here due to this health IT *system's* specific configuration or use of *component*.

Figure C.3 — *Manufacturer security* pattern

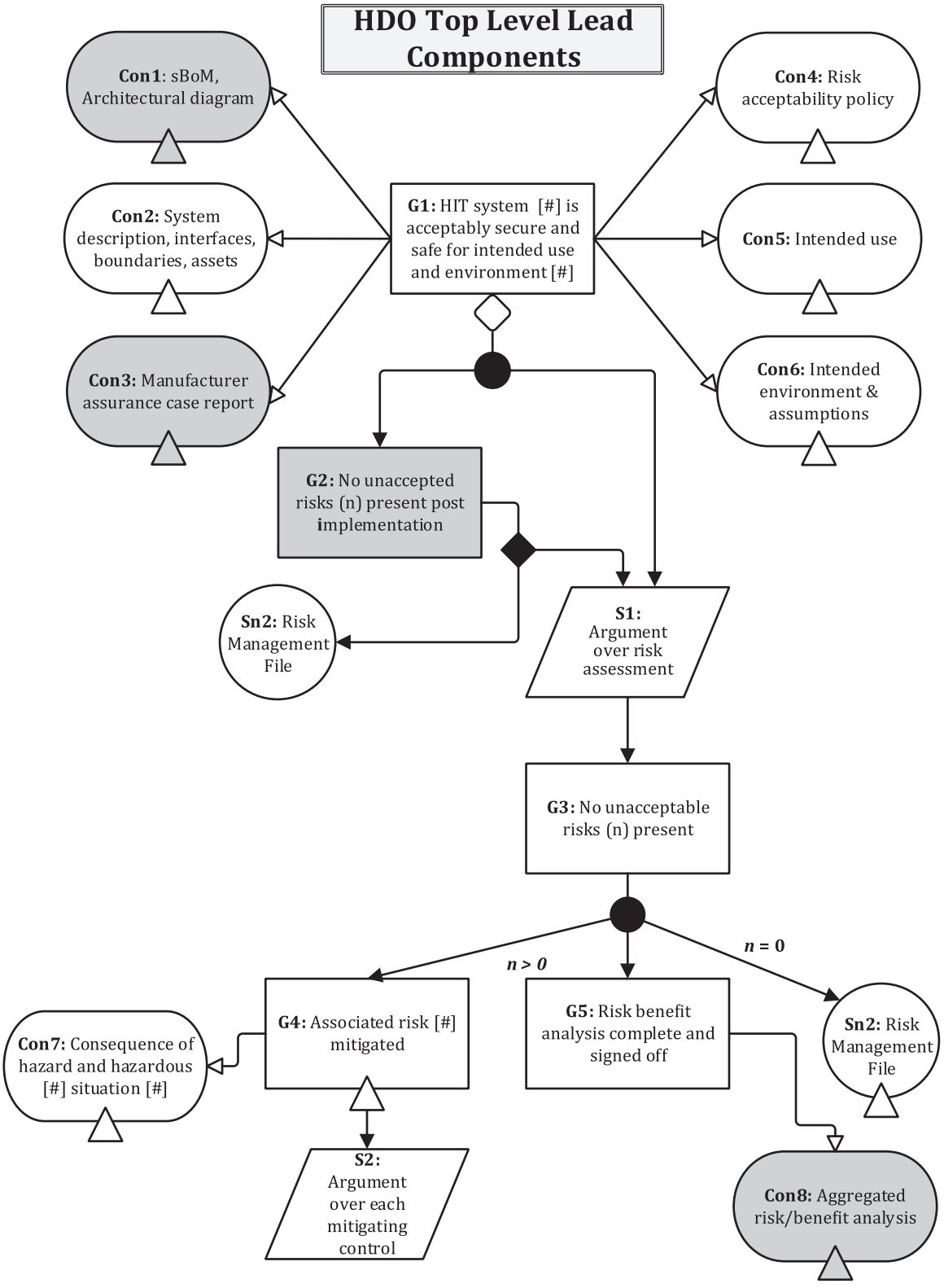
b) ***Healthcare Delivery Organization* (*HDO*) patterns**

Figure C.4 and Figure C.5 demonstrate typical *assurance case* patterns for a *health IT system* being implemented at a *healthcare delivery organization*.

Figure C.4 shows the top-level lead in pattern, where the appropriate level of information is provided by the *manufacturer* through an *assurance case* report as an important input (CON4) to the *HDO's assurance case* and *risk management processes*. This information should be considered a summary of the overall *assurance case*, structured in a pattern that can be interpreted easily by the next *risk* owner and can then be incorporated into the larger *assurance case* of the next *risk* owner.

Figure C.5 then illustrates how the *HDO* can carry out its parallel *safety* and *security assurance case* activities in order to manage the interdependence of the two properties and take into account the relevant aspects of the sociotechnical ecosystem in which the *health IT system* is being implemented

These same patterns are executed at each stage (acquisition through to *implementation* and decommissioning) with the information from each stage and *role* being passed to the next one. While the activities at each stage can be contracted to a third party (e.g. an *integrator*), the *HDO* ensures that the *safety assurance case* is augmented at each stage so that their *safety* and *security risks* are managed across the *life cycle* through good two-way communication between the respective parties and *roles* involved.



GSN Construct	Description
CON1	Establishes that the *HDO assurance case* considers the over-arching *health IT infrastructure* it is being integrated into.
CON3	Establishes that the *manufacturer's assurance case* report is considered and evaluated by the *HDO* in their own *risk management process*.
G2	Establishes the *HDO assurance case* addresses the *risk* associated with the integration of the *health IT system* within the wider *health IT infrastructure*.

GSN Construct	Description
CON8	Establishes that the *HDO* evaluates the aggregate *risk* vs benefit across the *organization*.

NOTE This pattern mirrors *manufacturer* (Figure C.1) but with the four important further elements highlighted.

Figure C.4 — *HDO* top level lead *components*

The subsequent element of the pattern (Figure C.5) mirrors that of the *manufacturer organization* (Figure C.2 and Figure C.3) emphasizing the importance of an integrated approach to *safety* and *security*:

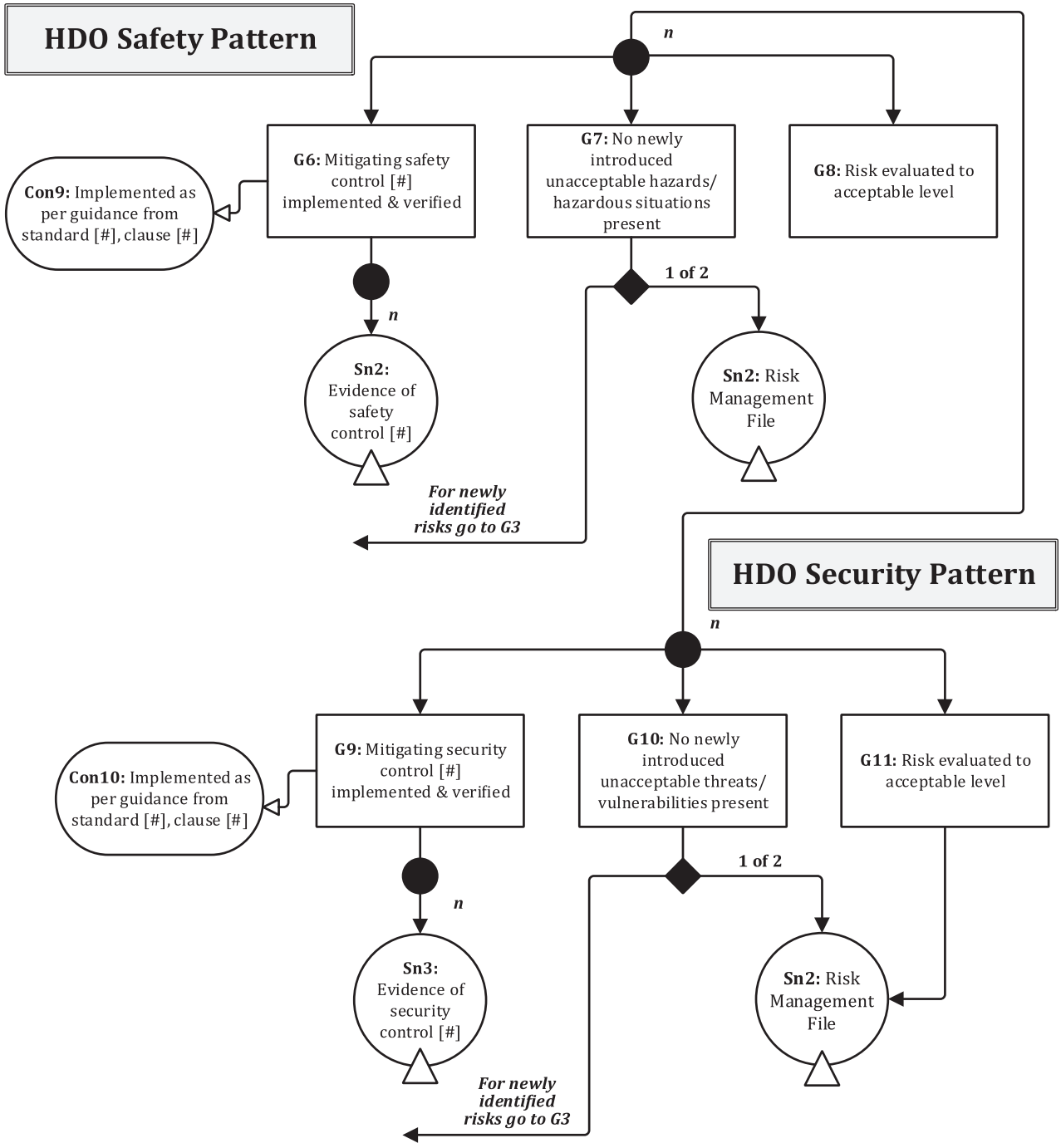


Figure C.5 — *HDO safety & security* pattern

C.3 Guidance on developing *assurance cases*

a) **The argument**

An effective argument in an assurance case has the following characteristics:

— **Bounded**: claims of *safety* and/or *security* can only be made within a pre-defined context so it is important that the scope of the *health IT system* and its subsequent use is clearly established and communicated. Modification of the *health IT system* beyond this definition or alternative use of the *health IT system* can compromise the integrity of the argument.

— **Relevant**: the argument strategy has to be appropriate to the nature of the *health IT system* and its subsequent use. For example, an argument that is based on clinician *user* testing becomes weak if the *health IT system* is predominately used by patients rather than clinicians.

— **Comprehensible**: the principal purpose of the assurance case is to communicate the integrity of the *health IT system*. If the argument is complex it becomes difficult to understand and any *weaknesses*, gaps and contradictions cannot be identified.

— **Structured**: an organised and logically structured argument will aid comprehension, making the argument easier to understand.

— **Supported**: ultimately, the argument has to be supported by evidence that demonstrates that the objectives have been achieved.

Examples of arguments include the following:

— hazardous software *risks* have been identified;

— relevant *security threats* have been identified;

— controls have been put in place to manage these *risks* and *threats;*

— mechanisms are in place to monitor the performance of the controls and the *system* on an on-going basis.

b) **The evidence**

To be effective the evidence provided in an assurance case should have the following qualities:

— **Traceable (argument)**: the inclusion of evidence in an assurance case supports the argument. So, the relationship between the argument and evidence is explained.

— **Relevant**: the evidence being included in support of the argument is appropriate and justified. For example, citing testing as a means to identify all foreseeable *hazards* is flawed.

— **Complete**: ultimately, the assurance case includes and demonstrates that all required evidence supporting the assurance case has been created.

— **Verified**: the *effectiveness* of the evidence in supporting the assurance case is demonstrated. e.g. all test requirements have been passed.

— **Available**: evidence is retained and accessible to support the assurance case throughout the life of the *health IT system*.

Examples of evidence include:

— tests

— analysis

— reviews

— expert judgement, and

— conformance with best practice

Other best practices that can assist in creating and maintaining effective *assurance cases* include the following:

— **Assume the *system* is not safe: "**Prove" all assumptions and claims. Challenge with "what if".

— **Avoid the trap of assuming the conclusion (the *system* is safe)**: Establish the assurance argument early in the *life cycle* and use it to drive evidence requirements rather than reverse engineering an assurance case from the available evidence**.**

— **Define key *safety* and *security* concepts such as *Hazard*, Cause, Control, *Threat*, *Vulnerability* and Effect**: Using terms consistently with agreed understanding of their meaning will aid in the comprehensibility of the assurance case and prevent misinterpretations.

— **Involve the right mix of personnel from the onset**: Teams that are comprised of members with different knowledge, experience, and competency help to create a more robust and complete assurance case.

— **Apply common sense**: It is unlikely that all aspects of the *system* are *safety*-related or *threat*-sensitive. By applying common sense, the team can identify the areas which pose greatest *risk* and subsequently focus attention there.

— **Plan ahead**: Create a route map to organise work activities, including a *risk management* plan.

— **Avoid obscure language**: Keep language simple and to the point.

c) **Assurance case reports**

The assurance case report is a physical document summarizing key elements of the assurance case, referencing all supporting material in a clear, comprehensible and concise format. Since its primary purpose is to communicate the relevant information for a particular purpose, it should summarize the relevant information for the stakeholder audience it is targeted to.

As the underlying assurance case continues to evolve during the *health IT system life cycle*, there is a need to issue assurance case reports in support of key milestones. The assurance case report can be used to communicate information relating to ongoing *risk management* across *roles* and organizational boundaries during the *life cycle* of the *health IT system*. The issuance of assurance case reports will be dictated by the *health IT system* development *life cycle* being followed, as defined in the *risk management* plan.

As indicated in Clause C.1, the *manufacturer's* assurance case report should be made available to the deploying *healthcare delivery organization*. This deliverable is a key input into the *HDO's risk management* activities.

The *manufacturer* should work in close collaboration with *HDOs* following delivery in order to ensure safe and effective deployment of the *health IT system*. Such relationships will minimise the likelihood of unanticipated issues occurring and ensure that any *risk controls* that the *manufacturer* is dependent on the *HDO* to implement are clearly communicated. The *HDO* in turn should communicate issues they encounter concerning the design or documentation of the *health IT system* throughout its *life cycle* back to the *manufacturer* for potential remediation.

Bibliography

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

[2] ISO 9000, *Quality management systems — Fundamentals and vocabulary*

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

[4] ISO 9001:2015, *Quality management systems — Requirements*

[5] ISO 13372:2012, *Condition monitoring and diagnostics of machines — Vocabulary*

[6] ISO 13485, *Medical devices — Quality management systems — Requirements for regulatory purposes*

[7] ISO 13940:2015, *Health informatics — System of concepts to support continuity of care*

[8] ISO/TS 13972:2015, *Health informatics — Detailed clinical models, characteristics and processes*

[9] ISO 14971:2019, *Medical devices — Application of risk management to medical devices*

[10] ISO/TS 20405:2018, *Health informatics — Framework of event data and reporting definitions for the safety of health software*

[11] ISO 20417[1)], *Medical devices — Information to be supplied by the manufacturer*

[12] ISO/TS 27790:2009, *Health informatics — Document registry framework*

[13] ISO 27799:2016, *Health informatics — Information security management in health using ISO/IEC 27002*

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

[15] ISO 80001 (all parts), *Application of risk management for IT-networks incorporating medical devices*

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

[17] ISO/IEC Guide 63:2019, *Guide to the development and inclusion of aspects of safety in International Standards for medical devices*

[18] ISO/IEC 2382:2015, *Information technology — Vocabulary*

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

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

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

[22] ISO/IEC 20000-1:2018, *Information technology — Service management — Part 1: Specification*

[23] ISO/IEC/TS 22237-7:2018, *Information technology — Data centre facilities and infrastructures — Part 7: Management and operational information*

[24] ISO/IEC 27032:2012, *Information technology — Security techniques — Guidelines for cybersecurity*

[25] ISO/IEC 27039:2015, *Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)*

1) Under preparation. Stage at the time of publication: ISO/FDIS 20417:2020.

[26] ISO/IEC 27701:2019, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

[27] ISO/HL7 21731:2006, *Health informatics — HL7 version 3 — Reference information model — Release 1 (Withdrawn)*

[28] IEC Guide 120:2018, *Security aspects — Guidelines for their inclusion in publications*

[29] IEC 61907:2009, *Communication network dependability engineering*

[30] IEC 62304, *Medical device software — Software life cycle processes*

[31] IEC 62366-1:2015, *Medical devices — Part 1: Application of usability engineering to medical devices*

[32] IEC 80001 (all parts), *Application of risk management for IT-networks incorporating medical devices*

[33] IEC 80001-1:2010, *Application of risk management for IT-networks incorporating medical devices — Part 1: Roles, responsibilities and activities*

[34] IEC/TR 80001-2-2:2012, *Application of risk management for IT-networks incorporating medical devices — Part 2-2: Guidance for the communication of medical device security needs, risks and controls*

[35] IEC/TR 80001-2-8:2016, *Application of risk management for IT-networks incorporating medical devices — Part 2-8: Application guidance — Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2*

[36] IEC/TR 80001-2-9:2017, *Application of risk management for IT-networks incorporating medical devices — Part 2-9: Application guidance — Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities*

[37] IEC 82304-1, *Health software — Part 1: General requirements for product safety*

[38] AAMI, (PS) HIT1000-1:2018, Safety and effectiveness of health software and systems—Part 1: Fundamental concepts, principles, and requirements for patient safety (Available at: https://webstore.ansi.org/Standards/AAMI/AAMIHIT1000PS2018)

[39] Canada Health Infoway, 2020. Change management toolkit: Leading change in health [viewed 2020-04-27]. Available from https://www.infoway-inforoute.ca/en/resource-centre/toolkits/change-management

[40] IETF RFC 4949, 2007. *Internet Security Glossary, Version 2 [viewed 2020-04-27]*. Available from: https://tools.ietf.org/html/rfc4949

[41] International Medical Device Regulators Forum (IMDRF), 2013. Software as a Medical Device (SaMD): Key Definitions [viewed 2020-04-27]. Available from http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf

[42] CNSSI, No. 4009, 2015. Committee on National Security Systems (CNSS) Glossary [viewed 2020-04-27]. Available from https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

[43] Committee on Patient Safety and Health Information Technology, Institute of Medicine, 2011. Health IT and Patient Safety: Building Safer Systems for Better Care. Washington (DC): National Academies Press (US).

[44] Magrabi F, Baker M, Sinha I, Ong MS, Harrison S, Kidd MR et al. , Clinical safety of England's national programme for IT: A retrospective analysis of all reported safety events 2005 to 2011. International Journal of Medical Informatics, 2015, **84**(3), 198.

[45] Makeham M, Magrabi F, Hibbert P, Hardie R, 2017. Literature review and environmental scan on approaches to the review and investigation of Health-IT related patient safety incidents. Sydney: ACSQHC.

[46] Neily J., Mills P.D., Young-Xu Y. et al. , Association between implementation of a medical team training program and surgical mortality. JAMA, 2010, **304**(15), 1693.

[47] Ronquillo J. G., Erik Winterholler J., Cwikla K., Szymanski R., Levy C. 2018. Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. *JAMIA open*, **1**(1), 15.

[48] The Assurance Case Working Group, 2018. Goal Structuring Notation Community Standard, Version 2 (SCSC-141B) [viewed 2020-04-2020]. Available from https://scsc.uk/scsc-141B

[49] ISO/IEC 20000 (all parts), *Information technology — Service management*

[50] Standard Computer Dictionary IEEE, A Compilation of IEEE Standard Computer Glossaries," in IEEE Std 610, vol., no., pp.1-217, 18 Jan. 1991[2)]

2) Withdrawn.

ICS 35.240.80

Price based on 61 pages