

American National Standard



ANSI/AAMI SW96:2023

Standard for medical device
security—Security risk
management for device
manufacturers

Standard for medical device security—Security risk management for device manufacturers

Approved 21 December 2022 by
AAMI

Approved 13 January 2023 by
American National Standards Institute, Inc.

Abstract: Provides requirements on methods to perform security risk management for a medical device in the context of the safety risk management process required by ISO 14971. This document is intended to be used in conjunction with AAMI TIR57 and AAMI TIR97.

Keywords: medical device, information security, security risk management

AAMI Standard

This Association for the Advancement of Medical Instrumentation (AAMI) standard implies a consensus of those substantially concerned with its scope and provisions. The existence of an AAMI standard does not in any respect preclude anyone, whether they have approved the standard or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standard. AAMI standards are subject to periodic review, and users are cautioned to obtain the latest editions.

CAUTION NOTICE: This AAMI standard may be revised or withdrawn at any time. AAMI procedures require that action be taken to reaffirm, revise, or withdraw this document no later than five years from the date of publication. Interested parties may obtain current information on all AAMI standards by calling or writing AAMI.

All AAMI standards, recommended practices, technical information reports, and other types of technical documents developed by AAMI are voluntary, and their application is solely within the discretion and professional judgment of the user of the document. Occasionally, voluntary technical documents are adopted by government regulatory agencies or procurement authorities, in which case the adopting agency is responsible for enforcement of its rules and regulations.

Published by

AAMI
901 N. Glebe Road, Suite. 300
Arlington, VA 22203
www.aami.org

© 2023 by the Association for the Advancement of Medical Instrumentation

All Rights Reserved

This publication is subject to copyright claims of AAMI. No part of this publication may be reproduced or distributed in any form, including an electronic retrieval system, without the prior written permission of AAMI. All requests pertaining to this document should be submitted to AAMI. It is illegal under federal law (17 U.S.C. § 101, et seq.) to make copies of all or any part of this document (whether internally or externally) without the prior written permission of the Association for the Advancement of Medical Instrumentation. Violator's risk legal action, including civil and criminal penalties, and damages of \$100,000 per offense. For permission regarding the use of all or any part of this document, visit the [Copyright Clearance Center](#).

Printed in the United States of America

ISBN 978-1-57020-862-1

Contents

Page

Committee representation.....	iv
Foreword.....	vi
Introduction	vii
1 Scope.....	1
2 Normative references.....	2
3 Terms and definitions.....	2
4 General requirements for <i>security risk management</i>	9
5 <i>Security risk analysis</i>	13
6 <i>Security risk evaluation</i>	15
7 <i>Security risk control</i>	15
8 Evaluation of overall <i>security residual risk acceptability</i>	18
9 <i>Security risk management review</i>	19
10 Production and <i>post-production</i> activities.....	19

Annexes

Annex A (informative) Rationale.....	24
Annex B (informative) The similarities and differences between <i>security</i> and <i>safety risk management</i>	25
Annex C (informative) <i>Security risk management</i> report.....	33
Annex D (informative) <i>Threat</i> modeling.....	39
Annex E (informative) Third-Party Service Organizations and <i>Security</i>	44
Annex F (informative) <i>Security risk</i> scoring based on <i>likelihood of occurrence</i>	45
Bibliography	49

Figures

Figure 1—Schematic representation of the <i>security risk management</i> process.....	10
Figure 2—Relationships between the <i>security risk</i> and <i>safety risk management</i> processes	18
Figure B.1—Mapping of IEC 80001-1 definition of <i>harm</i> to Figure 2, AAMI TIR57	27
Figure B.2—CVSS Scoring Metric Groups.....	30
Figure B.3—Relationship between <i>safety</i> and usability <i>risk analysis</i>	31
Figure B.4—Interrelationship between <i>safety</i> , usability, and <i>security</i>	31
Figure D.1—Asset oriented model in AAMI TIR57	42
Figure D.2— <i>Threat Actor</i> Methodology.....	43
Figure F.1—Reference Model (adapted from Figure E.1, ISO 14971:2007, and Figure 3, NIST SP 800-30 Rev. 1)	46

Committee representation

Association for the Advancement of Medication Instrumentation

AAMI Medical Device Security Working Group

This AAMI American National Standard (ANS) was developed and approved by the AAMI Medical Device Security Working Group.

At the time this document was published, the **AAMI Medical Device Security Working Group** had the following members:

Cochairs: Brian Fitzgerald
Michael Seeberger

Members: Daniel Black, ResMed Inc.
Ryan Burke, AJW Technology Consultants Inc
Nick Chozos, Adelard LLP
Martin Crnkovich, Fresenius Medical Care
David Deaven, GE Healthcare
Cody DeGroot, Hennepin Healthcare System
Stephanie Domas, MedSec
Sherman Eagles, SoftwareCPR
Charles Farlow, Farlow Systems Consulting, LLC
Brian Fitzgerald, FDA/CDRH
Alex Forward, SunTech Medical Inc
Alan Fryer, Micro Systems Engineering Inc
Kevin Fu, Archimedes Center for Healthcare and Device Security
John Giantsidis, CyberActa Inc
Stephen Grimes, ABM Healthcare Services
David Guffrey, Mass General Brigham
Bob Haack, Karl Storz Endoscopy
Robert Haack, Johnson & Johnson
Christopher Howard, Medical Sensor Systems, Inc.
Michael Jaffe, Cardiorespiratory Consulting LLC
Michelle Jump, MedSec
Joshua Kim, Hill-Rom Holdings
Matthew Kirkwood, Smiths Medical
Adam Lacy, Stryker Instruments Division
Juuso Leinonen, ECRI Institute
Yimin Li, Abbott Laboratories
Dan Lyon, Synopsys Inc
Matthew McKenna, Draeger Medical Systems Inc.
Vidya Murthy, MedCrypt
Scott Nichols, Beckman Coulter Inc.
Susumu Nozawa, Siemens Healthineers
Ojonimi Ocholi, Medtronic Inc
Brodie Pedersen, Borderless Compliance LLC
Andrea Ruth, ALR Consulting LLC
Michael Seeberger, Boston Scientific Corporation
Eirene Shipkowitz Smith, Baxter Healthcare Corporation
Jason Shutt, Olympus America Inc
Nick Sikorski, Deloitte Advisory
Chaitanya Srinivasamurthy, ICU Medical Inc
Sandra Stuart, Kaiser Foundation Health Plan/Hospitals
Eugene Vasserman, Kansas State University
David Vershum, Cantel Inc
Fubin Wu, GessNet
Daidi Zhong, Chongqing University
Charles Zinsmeyer, 3M Health Care

Alternates: Alireza Ashani, Amgen Inc
Robert Banta, Eli Lilly & Company
Justin Bushko, AJW Technology Consultants Inc
John Dwyier, Onclave Network Inc
Phillip Englert, Deloitte Advisory
Dawn Flakne, Micro Systems Engineering Inc
Clark Fortney, Battelle Memorial Institute
Edwin Heierman, Abbott Laboratories
Curtice Huntington, Smiths Medical
Mitchell Kiklas, 3M Health Care
Rakesh Paruthikkat, STERIS
Sagar Patel, Battelle Memorial Institute
Chris Reed, Medtronic Inc Campus
Scott Robertson, Kaiser Foundation
Mark Rohlwing, ICU Medical Inc
Lisa Simone, FDA/CDRH
Robert Smigielski, B Braun of America Inc
Varun Verma, Philips
Loren Walkington, Cardinal Health
Grace Wiechman, Boston Scientific Corporation
Nicole Zuk, Siemens Healthineers

Liaisons: Keith Anderson, Smiths Medical
Pat Baird, Philips
Tatiana Correia, 3M Health Care
Darren Dahlin, Cantel Inc
Anura Fernando, UL LLC
Zack Hornberger, Medical Imaging & Technology Alliance (MITA) a Division of NEMA
Kenneth Hoyme, Boston Scientific Corporation
Ujjwal Jain, Illumina Incorporated
Tara Larson, Abbott Laboratories
Jyh-Shyan Lin, DexCom Inc
Paul Matsumura, SunTech Medical Inc
Avital Merl, Becton Dickinson & Company
Komala Mullapudi, DexCom Inc
David Osborn, Philips
Robert Phillips, Siemens Healthineers
Umesh Shah, Abbott Laboratories
Donna Walsh, FDA/CDRH

NOTE Participation by federal agency representatives in the development of this document does not constitute endorsement by the federal government or any of its agencies.

Foreword

This document was developed by the AAMI Medical Device Security Working Group.

The challenge of managing *security risks* for *medical devices* throughout their *life cycle* is becoming more complex. To develop *medical devices* and systems cost effectively, the use of a larger set of commercial third-party components during the development of a *medical device* is becoming more common, particularly for *medical devices* that are intended to be connected to networks. The result is that the overall *security risk* for a *medical device* evolves over time even if the *medical device* does not change. Knowledge of new *vulnerabilities* and *threats* can originate from multiple sources. *Manufacturers* need to be prepared to receive *vulnerability* information, actively seek information on new *threats*, assess *risk*, and take the appropriate action.

Accordingly, *security risk management* of *medical devices* is a total product *life cycle* activity.

The objective of this document is to specify requirements based on the guidance provided in the subordinate AAMI TIR57 [3] and AAMI TIR97 [4] on how *medical device manufacturers* should manage *security risk* throughout the *life cycle* of a *medical device* within the *risk management* framework defined by ISO 14971.

The following verbal forms are used within AAMI documents to distinguish requirements from other types of provisions in the document:

- “shall” and “shall not” are used to express requirements;
- “should” and “should not” are used to express recommendations;
- “may” and “may not” are used to express permission;
- “can” and “cannot” are used as statements of possibility or capability;
- “must” is used for external constraints or obligations defined outside the document; “must” is not an alternative for “shall.”

Suggestions for improving this document are invited. Comments and suggested revisions should be sent to Standards, AAMI, 901 N. Glebe Road, Suite 300, Arlington, VA 22203 or standards@aami.org.

Introduction

ISO 14971 specifies a process for *risk management* of *medical devices*, including software as a *medical device* and in vitro diagnostic (IVD) *medical devices*. The process described intends to assist *manufacturers of medical devices* to identify the *hazards* associated with the *medical device*, to estimate and evaluate the associated *risks*, to control these *risks*, and to monitor the *effectiveness* of the controls (see Clause 1 of ISO 14971).

This document was developed to provide additional guidance and requirements specific to the unique handling of *medical device security risks*. AAMI TIR57 [3] provides guidance for addressing *security risk*, primarily during the design *life cycle* phase, within the *risk management* framework defined by ISO 14971. AAMI TIR97 [4] provides additional guidance on the management of postmarket *security risk* and is complimentary to AAMI TIR57 [3]. While TIR 97 and TIR 57 are technical information reports, this document is a standard that provides specific requirements for managing *security* related *risk* across the total product *life cycle* but within the *risk management* framework defined by ISO 14971.

Following the approach developed in AAMI TIR57 [3], the definition of *harm* is considered from the perspective of ISO 14971. Also considered is *harm* from healthcare information technology (IT) standards, such as the ANSI/AAMI/IEC 80001 family. Because a *risk management* process that narrowly focuses on the traditional “physical injury or damage” definition can limit the scope of *security risk management*, this document incorporates the broader considerations that *risks* include effects outside the traditional scope of patient physical *harm*, and can include “reduction of *effectiveness*,” and “breach of *data and systems security*” as extended in the ANSI/AAMI/IEC 80001 family of standards [6]. The relationship illustrated in AAMI TIR57 [3], Figure 2, “A Venn diagram showing the relationship between *security* and *safety risks*” is equally applicable to concepts presented in this document. Annex B provides additional background about the similarities and differences between *security* and *safety risk management*.

ISO/TR 24971 [23] describes a “production and *post-production* activities” that consist of three processes:

- information collection (Subclause 10.2);
- information review (Subclause 10.3); and
- actions (Subclause 10.4).

This document complements each of these processes by addressing the unique challenges associated with specifying and maintaining the *security* of a *medical device*.

The following supporting annexes are provided:

- Annex A: Rationale;
- Annex B: Similarities and differences between *safety risk management* and *security risk management*;
- Annex C: *Security risk management* report;
- Annex D: *Threat* modeling.
- Annex E: Third-Party Service Organizations and *Security*.
- Annex F: *Security risk* scoring based on *likelihood of occurrence*

Standard for medical device security—Security risk management for device manufacturers

1 Scope

This document provides requirements and guidance when addressing design, production and *post-production security risk management* for medical devices within the *risk management* framework defined by ISO 14971.

This document is intended to assist *manufacturers* and other users of the standard with the following:

- identifying *threats*, *vulnerabilities*, and *assets* associated with *medical devices* and their components and supply chain vendors;
- estimating and evaluating associated *security risks*;
- determining appropriate *security risk controls* to reduce *security risks*;
- verifying and monitoring the *effectiveness* of the *security risk controls*;
- establishing an enterprise-wide process to manage *security post-production* interactions with users and other stakeholders that ensures *security of medical devices* and systems used to provide medical care;
- creating design features that enable production and *post-production* management of *security risk* and effective integration with healthcare delivery organization (HDO) network *security* policies and technologies, or other operational contexts;
- coordinating communications with HDOs for *security risks*;
- understanding and communicating the *security* expectations from *manufacturers* to those who deploy their *medical devices* in a user environment;
- implementing processes to manage and monitor fielded *medical devices* containing either (1) traditional software (including firmware), (2) programmable logic, and (3) hardware for *security vulnerabilities*;
- implementing *security risk management* processes to 1) assess *security risk* in order to decide when action is required and 2) coordinate with *safety risk management* processes;
- coordinating with HDOs on *security risk management* activities;
- developing, implementing, and operationalizing a *coordinated vulnerability disclosure* process;
- implementing processes to manage *medical device security* patching; and
- planning for *medical device* retirement.

This document is applicable to the entire *life cycle* of a *medical device* including design, production, and *post-production* phases. *End of Support (EOS)* and *End of Guaranteed Support (EOGS)* are milestones in the *post-production* phase of the *medical device* and may vary according to differing market and jurisdictional factors.

This document expands on the information provided in Clause 10 “Production and *post-production* activities” of ISO/TR 24971 [23] by highlighting the need for proactive monitoring to assess *threats* and detect *vulnerabilities*. It references the coordinated *safety/security risk assessment* approach that was presented in Clause 9 of AAMI TIR57 [3], “Production and *post-production* information.”

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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/>.

3.1

accompanying documentation

materials accompanying a *medical device* (3.25) and containing information for the user of those accountable for the installation, use, maintenance, decommissioning and disposal of the *medical device* (3.25), particularly regarding safe use

NOTE 1 to entry: The *accompanying documentation* can consist of the instructions for use, technical description, installation manual, quick reference guide, etc.

NOTE 2 to entry: *Accompanying documentation* is not necessarily a written or printed document but could involve auditory, visual, or tactile materials and multiple media types.

[SOURCE: ISO 14971:2019, 3.1]

3.2

asset

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

[SOURCE: ISO/IEC 27032:2012, 4.6, modified – “anything” has been replaced by “physical entity or digital entity” at the beginning of the definition.]

3.3

attack

attempt to destroy, expose, alter, disable, steal, or gain unauthorized access to or make unauthorized use of an *asset* (3.2)

[SOURCE: ISO/IEC 27000:2018, 3.2]

3.4

authentication

provision of assurance that a claimed characteristic of an entity is correct

[SOURCE: ISO/IEC 27000:2018, 3.5]

3.5

authorization

granting of privileges, which includes the granting of privileges to access data and functions

Note 1 to entry: Derived from ISO 7498-2: the granting of rights [8], which includes the granting of access based on access rights.

[SOURCE: ISO 27789:2013, 3.12]

3.6

availability

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

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.7

benefit

positive impact or desirable outcome of the use of a *medical device* (3.25) on the health of an individual, or a positive impact on patient management or public health

Note 1 to entry: *Benefits* can include positive impact on clinical outcome, the patient's quality of life, outcomes related to diagnosis, positive impact from diagnostic devices on clinical outcomes, or positive impact on public health.

[SOURCE: ISO 14971:2019, 3.2]

3.8

compensating risk control measure

compensating control

specific type of *risk control* (3.34) measure deployed in lieu of, or in the absence of, *risk control* (3.34) measures implemented as part of the device's design

Note 1 to entry: A *compensating risk control measure* could be permanent or temporary (e.g., until the *manufacturer* can provide an update that incorporates additional *risk control* measures).

[SOURCE: AAMI TIR97:2019, 2.2]

3.9

confidentiality

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

[SOURCE: ISO/IEC 27000:2018, 3.10]

3.10

coordinated vulnerability disclosure

CVD

process through which researchers and other interested parties work cooperatively with a *manufacturer* (3.24) in finding solutions that reduce the *risks* (3.31) associated with disclosure of *vulnerabilities* (3.47)

Note 1 to entry: This process encompasses actions such as reporting, coordinating, and publishing information about a *vulnerability* and its resolution.

[SOURCE: AAMI TIR97:2019, 2.3]

3.11

data and systems security

operational state of a *medical device* (3.25) in which information assets (3.2) (data and systems) are reasonably protected from degradation of *confidentiality* (3.9), *integrity* (3.20), and *availability* (3.6)

[SOURCE: ANSI/AAMI/IEC 80001-1:2010, 2.5, modified - "medical IT-network" has been replaced with "*medical device*," Note 1 to entry and Note 2 to entry wave been redacted.]

3.12

effectiveness

ability to produce the intended result for the patient and the care provider

[SOURCE: ANSI/AAMI/IEC 80001-1:2010, 2.6, modified - "responsible organization" has been replaced with "care provider."]

3.13

end of guaranteed support

EOGS

life cycle (3.22) stage that begins when the *manufacturer* (3.24) no longer guarantees full support

Note 1 to entry: During this life cycle stage, there can be some level of support available by the *manufacturer*, but without a guarantee that the *medical device* can be maintained to its original specification and performance.

[SOURCE: AAMI TIR97:2019, 2.5, modified – “point at after which” has been replaced by “life cycle (3.22) stage that begins when”.]

3.14

end of support

EOS

life cycle (3.22) stage that begins when the *manufacturer* (3.24) terminates all service support activities

Note 1 to entry: Service support does not extend beyond this point.

[SOURCE: AAMI TIR97:2019, 2.6, modified – “point after which” has been replaced by “life cycle (3.22) stage that begins when”.]

3.15

exploit

defined way to breach the *security* (3.39) of information systems through *vulnerability* (3.47)

[SOURCE: ISO/IEC 27039:2015, 2.9]

3.16

harm

physical injury or damage to the health of people, or damage to property or the environment, or reduction in *effectiveness* (3.12), or breach of *data and systems security* (3.11)

[SOURCE: IEC 80001-1:2010, 2.8]

3.17

hazard

potential source of *harm* (3.16)

[SOURCE: ISO/IEC Guide 51:2014, 3.2]

3.18

hazardous situation

circumstance in which people, property or the environment is/are exposed to one or more *hazards* (3.17)

[SOURCE: ISO/IEC Guide 51:2014, 3.4]

3.19

information sharing and analysis organization

ISAO

any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of gathering, analyzing, communicating, disclosing, or voluntarily disseminating information in order to better understand *security* (3.39) problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the *availability* (3.6), *integrity* (3.20), and reliability thereof

Note 1 to entry: An ISAO communicates or discloses critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or an incapacitation problem related to critical infrastructure or protected systems.

Note 2 to entry: An ISAO voluntarily disseminates critical infrastructure information to its members, local and Federal Governments, or any other entities that may be of assistance. Similar organizations exist in other countries.

[SOURCE: AAMI TIR97:2019, 2.10]

3.20

integrity

property of accuracy and completeness

[SOURCE: ISO/IEC 27000:2018, 3.36]

3.21

intended use

use for which a product, process or service is intended according to the specifications, instructions, and information provided by the *manufacturer* (3.24)

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]

3.22

life cycle

series of all phases in the life of a *medical device* (3.25), from the initial conception to final decommissioning and disposal

[SOURCE: ISO/IEC Guide 63:2019, 3.5]

3.23

likelihood of occurrence

weighted factor based on a subjective analysis of the probability that a given *threat* (3.43) is capable of exploiting a given *vulnerability* (3.47)

Note 1 to entry: *Likelihood of occurrence* combines an estimate of the likelihood that the *threat event* will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the *threat event* results in adverse impacts).

[SOURCE: AAMI TIR57:2016, 2.16]

3.24

manufacturer

natural or legal person with responsibility for the design and/or manufacture of a *medical device* (3.25) with the intention of making the *medical device* (3.25) available for use, under his name, whether or not such a *medical device* (3.25) is designed and/or manufactured by that person himself or on his behalf by another person(s)

Note 1 to entry: The natural or legal person has ultimate legal responsibility for ensuring compliance with all applicable regulatory requirements for the *medical device* in the countries or jurisdictions where it is intended to be made available or sold unless this responsibility is specifically imposed on another person by the Regulatory Authority (RA) within that jurisdiction.

Note 2 to entry: The *manufacturer's* responsibilities are described in other GHTF guidance documents. These responsibilities include meeting both pre-market requirements and post-market requirements, such as adverse event reporting and notification of corrective actions.

Note 3 to entry: "Design and/or manufacture" may include specification development, production, fabrication, assembly, processing, packaging, repackaging, labelling, relabeling, sterilization, installation, or remanufacturing of a *medical device*; or putting a collection of devices, and possibly other products, together for a medical purpose.

Note 4 to entry: Any person who assembles or adapts a *medical device* that has already been supplied by another person for an individual patient, in accordance with the instructions for use, is not the *manufacturer*, provided the assembly or adaptation does not change the *intended use* of the *medical device*.

Note 5 to entry: Any person who changes the *intended use* of, or modifies, a *medical device* without acting on behalf of the original *manufacturer* and who makes it available for use under his own name, should be considered the *manufacturer* of the modified *medical device*.

Note 6 to entry: An authorized representative, distributor or importer who only adds its own address and contact details to the *medical device* or the packaging, without covering or changing the existing labelling, is not considered a *manufacturer*.

Note 7 to entry: To the extent that an accessory is subject to the regulatory requirements of a *medical device*, the person responsible for the design and/or manufacture of that accessory is considered to be a *manufacturer*.

[SOURCE: ISO/IEC Guide 63:2019, 3.6]

3.25

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* (3.24) to be used, alone or in combination, for human beings, for one or more of the specific medical purpose(s) of:

- diagnosis, prevention, monitoring, treatment, or alleviation of disease;
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury;
- investigation, replacement, modification, or support of the anatomy or of a physiological process;
- supporting or sustaining life;
- control of conception;
- disinfection of *medical devices* (3.25);
- 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 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]

3.26

password

string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access *authorization* (3.5)

[SOURCE: ISO/TR 22100-4:2018, 3.13]

3.27

post-production

part of the *life cycle* (3.22) of the *medical device* (3.25) after the design has been completed and the *medical device* (3.25) has been manufactured

EXAMPLES: Transportation, storage, installation, product use, maintenance, repair, product changes, decommissioning and disposal.

Note 1 to entry: The *post-production* phase includes devices manufactured and placed in inventory as well as those devices that have been shipped to customers and are subject to postmarket surveillance.

[SOURCE: ISO 14971:2019, 3.12, modified – Note 1 to entry has been added.]

3.28

predisposing condition

condition that exists within an organization, a mission/business process, enterprise architecture, or information system, including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more *threat events* (3.45), once initiated, will result in undesirable consequences or adverse impact to organizational operations and assets (3.2), individuals, or other organizations

Note 1 to entry: Identical to NIST definition (SP 800-30 Revision 1) [30] with the phrase “or the Nation” redacted.

[SOURCE: NIST SP 800-30 Revision 1 (2012)]

3.29

reasonably foreseeable misuse

use of a product or system in a way not intended by the *manufacturer* (3.24), but which can result from readily predictable human behavior

Note 1 to entry: Readily predictable human behavior includes the behavior of all types of users, 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]

3.30

residual risk

risk (3.31) remaining after *risk control* (3.34) measures have been implemented

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

3.31

risk

combination of the probability of occurrence of *harm* (3.16) and the *severity* (3.41) of that *harm* (3.16)

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

Note 2 to entry: For a *security* related *risk*, determining a statistically based probability is typically not possible. The use of a proxy such as exploitability or likelihood score is acceptable. Refer to Annex B.5.

[SOURCE: ISO/IEC Guide 63:2019, 3.10, modified – Note 2 to entry has been added.]

3.32

risk analysis

systematic use of available information to identify *hazards* (3.17) and to estimate the *risk* (3.31)

[SOURCE: ISO/IEC Guide 51:2014, 3.10]

3.33

risk assessment

overall process comprising a *risk analysis* (3.32) and a *risk evaluation* (3.35)

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

3.34

risk control

process in which decisions are made and measures are implemented by which *risks* (3.31) are reduced to, or maintained within, specified levels

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

3.35

risk evaluation

process of comparing the estimated *risk* (3.31) against given *risk* criteria to determine the acceptability of the *risk*

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

3.36

risk management

systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating, controlling, and monitoring *risk* (3.31)

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

3.37

risk management file

set of records and other documents that are produced by *risk management* (3.36)

[SOURCE: ISO 14971:2019, 3.25]

3.38

safety

freedom from unacceptable *risk* (3.31)

Note 1 to entry: In the context of this document, *safety* is associated with physical injury or damage to the health of people, or damage to property or the environment (i.e., a subset of *harm*).

[SOURCE: ISO/IEC Guide 63:2019, 3.16, modified — Note 1 to entry has been added.]

3.39

security

cybersecurity

state where information and systems are protected from unauthorized activities, such as access, use, disclosure, disruption, modification, or destruction to a degree that the *risks* (3.31) related to violation of *confidentiality* (3.9), *integrity* (3.20), and *availability* (3.6) are maintained at an acceptable level throughout the *life cycle* (3.22)

[SOURCE: ISO 81001-1:2021, 3.2.13]

3.40

security incident

a violation or imminent *threat* (3.43) of violation of *security* (3.39) policies, acceptable use policies, or standard *security* practices

[SOURCE: NIST SP 800-61 Rev. 2 (2012), modified – The term “computer” has been removed from the definition included in section 2.1.]

3.41

severity

measure of the possible consequences of a *hazard* (3.17)

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

3.42

state of the art

developed stage of technical capability at a given time as regards products, processes, and services, based on the relevant consolidated findings of science, technology, and experience

Note 1 to entry: The *state of the art* embodies what is currently and generally accepted as good practice in technology and medicine. The *state of the art* does not necessarily imply the most technologically advanced solution. The *state of the art* described here is sometimes referred to as the “generally acknowledged *state of the art*.”

[SOURCE: ISO/IEC Guide 63:2019, 3.18]

3.43

threat

potential for violation of *security* (3.39), which exists when there is a circumstance, capability, action, or event that could breach *security* and cause *harm* (3.16)

[SOURCE: ISO/IEC Guide 120:2018, 3.16]

3.44

threat actor

individual or a group posing a *threat* (3.43)

[SOURCE: NIST SP 800-150 (2016)]

3.45

threat event

event or situation that has the potential for causing undesirable consequences or impact

[SOURCE: NIST SP 800-30 Revision 1 (2012)]

3.46

threat source

intent and method targeted at the intentional exploitation of a *vulnerability* (3.47) or a situation and method that may accidentally trigger a *vulnerability* (3.47)

[SOURCE: FIPS 200 (2016)]

3.47

vulnerability

weakness of an *asset* (3.2) or control that can be exploited by one or more *threats* (3.43)

[SOURCE: ISO/IEC 27000:2018, 3.77]

4 General requirements for *security risk management*

4.1 *Security risk management process*

The *manufacturer* shall establish, implement, document, and maintain an ongoing *security risk management* process for:

- a) Identifying *assets* associated with a *medical device* and the *threats*, *vulnerabilities*, and their corresponding adverse impacts on those *assets*;
- b) estimating and evaluating the associated *risks*;
- c) controlling these *risks*;
- d) verifying the implementation of *security risk control* measures and monitoring their *effectiveness*; and
- e) communicating *risks* and mitigations to affected stakeholders.

The *security risk management* process should be coordinated with other *medical device risk management* processes such as human factors *risk management*, *safety risk management*, supply chain risk management, and others as applicable.

Figure 1 provides a schematic representation of the *security risk management* process and the ordering of the steps.

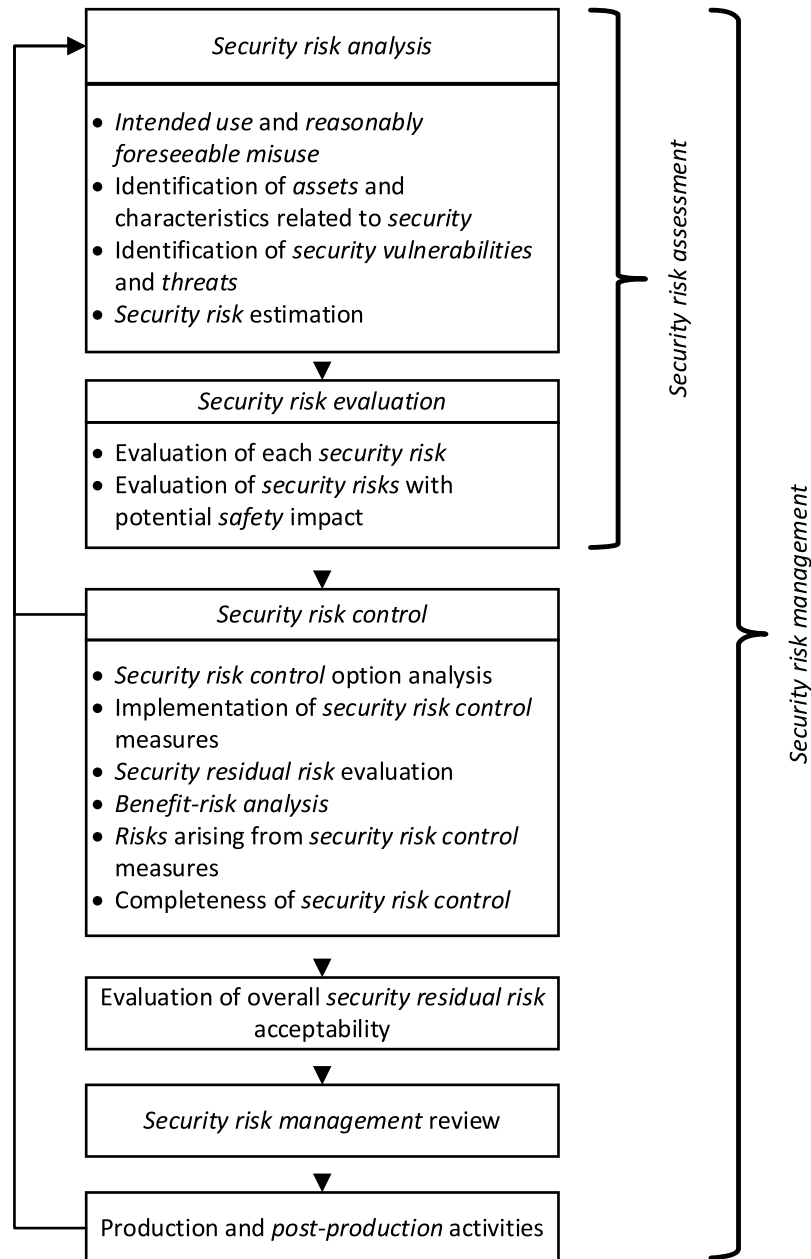


Figure 1—Schematic representation of the *security risk management* process

Adapted with permission from AAMI TIR57:2016/(R)2019; Principles for medical device security—Risk management. Arlington, VA: Association for the Advancement of Medical Instrumentation; Figure 1. © AAMI.

The *security risk management* process shall include the following elements:

- *security risk analysis*;
- *security risk evaluation*;
- *security risk control*;
- evaluation of overall *security residual risk* acceptability;
- *security risk management* review; and