INTERNATIONAL STANDARD

ISO 14971

Third edition
2019-12

Medical devices — Application of risk management to medical devices

Dispositifs médicaux — Application de la gestion des risques aux dispositifs médicaux

Reference number
ISO 14971:2019(E)

© ISO 2019



COPYRIGHT PROTECTED DOCUMENT

© ISO 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**

Introduction ... **vi**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 General requirements for *risk management* system ... **7**
4.1 ***Risk management process*** ... 7
4.2 Management responsibilities ... 8
4.3 Competence of personnel ... 9
4.4 ***Risk management*** plan ... 9
4.5 ***Risk management file*** ... 10

5 *Risk analysis* ... **10**
5.1 ***Risk analysis process*** ... 10
5.2 ***Intended use*** and ***reasonably foreseeable misuse*** ... 10
5.3 Identification of characteristics related to ***safety*** ... 11
5.4 Identification of ***hazards*** and ***hazardous situations*** ... 11
5.5 ***Risk estimation*** ... 11

6 *Risk evaluation* ... **12**

7 *Risk control* ... **12**
7.1 ***Risk control*** option analysis ... 12
7.2 Implementation of ***risk control*** measures ... 13
7.3 ***Residual risk*** evaluation ... 13
7.4 ***Benefit-risk*** analysis ... 14
7.5 ***Risks*** arising from ***risk control*** measures ... 14
7.6 Completeness of ***risk control*** ... 14

8 Evaluation of overall *residual risk* ... **14**

9 *Risk management* review ... **15**

10 Production and *post-production* activities ... **15**
10.1 General ... 15
10.2 Information collection ... 15
10.3 Information review ... 16
10.4 Actions ... 16

Annex A (informative) **Rationale for requirements** ... **17**

Annex B (informative) ***Risk management process*** **for *medical devices*** ... **26**

Annex C (informative) **Fundamental *risk* concepts** ... **30**

Bibliography ... **36**

© ISO 2019 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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 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).

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 by Technical Committee ISO/TC 210, *Quality management and corresponding general aspects for medical devices*, and IEC/SC 62A, *Common aspects of electrical equipment used in medical practice*.

This third edition cancels and replaces the second edition (ISO 14971:2007), which has been technically revised. The main changes compared to the previous edition are as follows:

— A clause on normative references has been included, in order to respect the requirements for fixed in Clause 15 of ISO/IEC Directives, Part 2:2018.

— The defined terms are updated and many are derived from ISO/IEC Guide 63:2019. Defined terms are printed in italic to assist the reader in identifying them in the body of the document.

— Definitions of *benefit*, *reasonably foreseeable misuse* and *state of the art* have been introduced.

— More attention is given to the *benefits* that are expected from the use of the *medical device*. The term *benefit-risk* analysis has been aligned with terminology used in some regulations.

— It is explained that the *process* described in ISO 14971 can be used for managing *risks* associated with *medical devices*, including those related to data and systems security.

— The method for the evaluation of the overall *residual risk* and the criteria for its acceptability are required to be defined in the *risk management* plan. The method can include gathering and reviewing data and literature for the *medical device* and for similar *medical devices* and similar other products on the market. The criteria for the acceptability of the overall *residual risk* can be different from the criteria for acceptability of individual *risks*.

— The requirements to disclose *residual risks* have been moved and merged into one requirement, after the overall *residual risk* has been evaluated and judged acceptable.

— The review before commercial distribution of the *medical device* concerns the execution of the *risk management* plan. The results of the review are documented as the *risk management* report.

© ISO 2019 – All rights reserved

— The requirements for production and *post-production* activities have been clarified and restructured. More detail is given on the information to be collected and the actions to be taken when the collected information has been reviewed and determined to be relevant to *safety*.

— Several informative annexes are moved to the guidance in ISO/TR 24971, which has been revised in parallel. More information and a rationale for the requirements in this third edition of ISO 14971 have been provided in Annex A. The correspondence between the clauses of the second edition and those of this third edition is given in Annex B.

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.

© ISO 2019 – All rights reserved

Introduction

The requirements contained in this document provide *manufacturers* with a framework within which experience, insight and judgment are applied systematically to manage the *risks* associated with the use of *medical devices*.

This document was developed specifically for *manufacturers* of *medical devices* on the basis of established principles of *risk management* that have evolved over many years. This document could be used as guidance in developing and maintaining a *risk management process* for other products that are not necessarily *medical devices* in some jurisdictions and for suppliers and other parties involved in the *medical device life cycle*.

This document deals with *processes* for managing *risks* associated with *medical devices*. *Risks* can be related to injury, not only to the patient, but also to the user and other persons. *Risks* can also be related to damage to property (for example objects, data, other equipment) or the environment.

Risk management is a complex subject because each stakeholder can place a different value on the acceptability of *risks* in relation to the anticipated *benefits*. The concepts of *risk management* are particularly important in relation to *medical devices* because of the variety of stakeholders including medical practitioners, the organizations providing health care, governments, industry, patients and members of the public.

It is generally accepted that the concept of *risk* has two key components:

— the probability of occurrence of *harm*; and

— the consequences of that *harm*, that is, how severe it might be.

All stakeholders need to understand that the use of a *medical device* involves an inherent degree of *risk*, even after the *risks* have been reduced to an acceptable level. It is well known that in the context of a clinical *procedure* some *residual risks* remain. The acceptability of a *risk* to a stakeholder is influenced by the key components listed above and by the stakeholder's perception of the *risk* and the *benefit*. Each stakeholder's perception can vary depending upon their cultural background, the socio-economic and educational background of the society concerned and the actual and perceived state of health of the patient. The way a *risk* is perceived also takes into account other factors, for example, whether exposure to the *hazard* or *hazardous situation* seems to be involuntary, avoidable, from a man-made source, due to negligence, arising from a poorly understood cause, or directed at a vulnerable group within society.

As one of the stakeholders, the *manufacturer* reduces *risks* and makes judgments relating to the *safety* of a *medical device*, including the acceptability of *residual risks*. The *manufacturer* takes into account the generally acknowledged *state of the art*, in order to determine the suitability of a *medical device* to be placed on the market for its *intended use*. This document specifies a *process* through which the *manufacturer* of a *medical device* can identify *hazards* associated with the *medical device*, estimate and evaluate the *risks* associated with these *hazards*, control these *risks*, and monitor the effectiveness of the controls throughout the *life cycle* of the *medical device*.

The decision to use a *medical device* in the context of a particular clinical *procedure* requires the *residual risks* to be balanced against the anticipated *benefits* of the *procedure*. Such decisions are beyond the scope of this document and take into account the *intended use*, the circumstances of use, the performance and *risks* associated with the *medical device*, as well as the *risks* and *benefits* associated with the clinical *procedure*. Some of these decisions can be made only by a qualified medical practitioner with knowledge of the state of health of an individual patient or the patient's own opinion.

For any particular *medical device*, other standards or regulations could require the application of specific methods for managing *risk*. In those cases, it is necessary to also follow the requirements outlined in those documents.

© ISO 2019 – All rights reserved

The verbal forms used in this document conform to the usage described in Clause 7 of the ISO/IEC Directives, Part 2:2018. For the purposes of this document, the auxiliary verb:

— "shall" means that compliance with a requirement or a test is mandatory for compliance with this document;

— "should" means that compliance with a requirement or a test is recommended but is not mandatory for compliance with this document;

— "may" is used to describe permission (e.g. a permissible way to achieve compliance with a requirement or test);

— "can" is used to express possibility and capability; and

— "must" is used to express an external constraint that is not a requirement of the document.

© ISO 2019 – All rights reserved

Medical devices — Application of risk management to medical devices

1 Scope

This document specifies terminology, principles and a *process* for *risk management* of *medical devices*, including software as a *medical device* and *in vitro diagnostic medical devices*. The *process* described in this document 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.

The requirements of this document are applicable to all phases of the *life cycle* of a *medical device*. The *process* described in this document applies to *risks* associated with a *medical device*, such as *risks* related to biocompatibility, data and systems security, electricity, moving parts, radiation, and usability.

The *process* described in this document can also be applied to products that are not necessarily *medical devices* in some jurisdictions and can also be used by others involved in the *medical device life cycle*.

This document does not apply to:

— decisions on the use of a *medical device* in the context of any particular clinical *procedure*; or

— business *risk management*.

This document requires *manufacturers* to establish objective criteria for *risk* acceptability but does not specify acceptable *risk* levels.

Risk management can be an integral part of a quality management system. However, this document does not require the *manufacturer* to have a quality management system in place.

NOTE Guidance on the application of this document can be found in ISO/TR 24971[9].

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/

3.1
accompanying documentation
materials accompanying a *medical device* (3.10) and containing information for the user or those accountable for the installation, use, maintenance, decommissioning and disposal of the *medical device* (3.10), 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.

© ISO 2019 – All rights reserved

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.

3.2
benefit
positive impact or desirable outcome of the use of a *medical device* (3.10) 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.

3.3
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
hazard
potential source of *harm* (3.3)

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

3.5
hazardous situation
circumstance in which people, property or the environment is/are exposed to one or more *hazards* (3.4)

Note 1 to entry: See Annex C for an explanation of the relationship between hazard and hazardous situation.

[SOURCE: ISO/IEC Guide 63:2019, 3.3, modified — Note 1 to entry added.]

3.6
intended use
intended purpose
use for which a product, *process* (3.14) or service is intended according to the specifications, instructions and information provided by the *manufacturer* (3.9)

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]

3.7
in vitro diagnostic medical device
IVD medical device
device, whether used alone or in combination, intended by the *manufacturer* (3.9) for the in vitro examination of specimens derived from the human body solely or principally to provide information for diagnostic, monitoring or compatibility purposes and including reagents, calibrators, control materials, specimen receptacles, software, and related instruments or apparatus or other articles

[SOURCE: ISO 18113-1:2009, 3.27, modified — NOTE deleted.]

3.8
life cycle
series of all phases in the life of a *medical device* (3.10), from the initial conception to final decommissioning and disposal

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

© ISO 2019 – All rights reserved

3.9
manufacturer
natural or legal person with responsibility for the design and/or manufacture of a *medical device* (3.10) with the intention of making the *medical device* (3.10) available for use, under his name, whether or not such a *medical device* (3.10) 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, relabelling, 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 authorised 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]

3.10
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* (3.9) 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* (3.10),

— 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 may be assisted in its 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:

© ISO 2019 – All rights reserved

— disinfection substances;

— aids for persons with disabilities;

— devices incorporating animal and/or human tissues;

— devices for in vitro fertilization or assisted reproduction technologies.

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

3.11
objective evidence
data supporting the existence or verity of something

Note 1 to entry: *Objective evidence* can be obtained through observation, measurement, test or by other means.

[SOURCE: ISO 9000:2015, 3.8.3, modified — Note 2 to entry deleted.]

3.12
post-production
part of the *life cycle* (3.8) of the *medical device* (3.10) after the design has been completed and the *medical device* (3.10) has been manufactured

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

3.13
procedure
specified way to carry out an activity or a *process* (3.14)

Note 1 to entry: *Procedures* can be documented or not.

[SOURCE: ISO 9000:2015, 3.4.5]

3.14
process
set of interrelated or interacting activities that use inputs to deliver an intended result

Note 1 to entry: Whether the "intended result" of a *process* is called output, product or service depends on the context of the reference.

Note 2 to entry: Inputs to a *process* are generally the outputs of other *processes* and outputs of a *process* are generally the inputs to other *processes*.

Note 3 to entry: Two or more interrelated and interacting *processes* in series can also be referred to as a *process*.

[SOURCE: ISO 9000:2015, 3.4.1, modified — Notes to entry 4, 5 and 6 are deleted.]

3.15
reasonably foreseeable misuse
use of a product or system in a way not intended by the *manufacturer* (3.9), 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, 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]

© ISO 2019 – All rights reserved

3.16
record
document stating results achieved or providing evidence of activities performed

Note 1 to entry: *Records* can be used, for example, to formalize traceability and to provide evidence of *verification*, preventive action and corrective action.

Note 2 to entry: Generally *records* need not be under revision control.

[SOURCE: ISO 9000:2015, 3.8.10]

3.17
residual risk
risk remaining after *risk control* (3.21) measures have been implemented

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

3.18
risk
combination of the probability of occurrence of *harm* (3.3) and the *severity* (3.27) of that *harm* (3.3)

[SOURCE: ISO/IEC Guide 63:2019, 3.10, modified — Note 1 to entry deleted.]

3.19
risk analysis
systematic use of available information to identify *hazards* (3.4) and to estimate the *risk* (3.18)

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

3.20
risk assessment
overall *process* (3.14) comprising a *risk analysis* (3.19) and a *risk evaluation* (3.20)

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

3.21
risk control
process (3.14) in which decisions are made and measures implemented by which *risks* (3.18) are reduced to, or maintained within, specified levels

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

3.22
risk estimation
process (3.14) used to assign values to the probability of occurrence of *harm* (3.3) and the *severity* (3.27) of that harm

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

3.23
risk evaluation
process (3.14) of comparing the estimated *risk* (3.18) against given *risk* (3.18) criteria to determine the acceptability of the *risk* (3.18)

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

3.24
risk management
systematic application of management policies, *procedures* (3.13) and practices to the tasks of analysing, evaluating, controlling and monitoring *risk* (3.18)

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

© ISO 2019 – All rights reserved

3.25
risk management file
set of *records* (3.16) and other documents that are produced by *risk management* (3.24)

3.26
safety
freedom from *unacceptable risk* (3.18)

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

3.27
severity
measure of the possible consequences of a *hazard* (3.4)

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

3.28
state of the art
developed stage of technical capability at a given time as regards products, *processes* (3.14) 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]

3.29
top management
person or group of people who directs and controls a *manufacturer* (3.9) at the highest level

[SOURCE: ISO 9000:2015, 3.1.1, modified — "An organization" replaced by "a *manufacturer*", Notes to entry deleted.]

3.30
use error
user action or lack of user action while using the *medical device* (3.10) that leads to a different result than that intended by the *manufacturer* (3.9) or expected by the user

Note 1 to entry: *Use error* includes the inability of the user to complete a task.

Note 2 to entry: *Use errors* can result from a mismatch between the characteristics of the user, user interface, task, or use environment.

Note 3 to entry: Users might be aware or unaware that a *use error* has occurred.

Note 4 to entry: An unexpected physiological response of the patient is not by itself considered *use error*.

Note 5 to entry: A malfunction of a *medical device* that causes an unexpected result is not considered a *use error*.

[SOURCE: IEC 62366-1:2015, 3.21, modified — Note 6 to entry deleted.]

3.31
verification
confirmation, through the provision of *objective evidence* (3.11), 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*.

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

© ISO 2019 – All rights reserved

[SOURCE: ISO/IEC Guide 63:2019, 3.19]

4 General requirements for *risk management* system

4.1 *Risk management process*

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

a) identifying *hazards* and *hazardous situations* associated with a *medical device*;

b) estimating and evaluating the associated *risks*;

c) controlling these *risks*, and

d) monitoring the effectiveness of the *risk control* measures.

This *process* shall apply throughout the *life cycle* of the *medical device*.

This *process* shall include the following elements:

— *risk analysis*;

— *risk evaluation*;

— *risk control*; and

— production and *post-production* activities.

Where a documented product realization *process* exists, it shall incorporate the appropriate parts of the *risk management process*.

NOTE 1 Product realization *processes* are described in, for example, Clause 7 of ISO 13485:2016[5].

NOTE 2 A documented *process* within a quality management system can be used to address *safety* in a systematic manner, in particular to enable the early identification of *hazards* and *hazardous situations* in complex *medical devices*.

NOTE 3 A schematic representation of the *risk management process* is shown in Figure 1. Depending on the specific *life cycle* phase, individual elements of *risk management* can have varying emphasis. Also, *risk management* activities can be performed iteratively or in multiple steps as appropriate to the *medical device*. Annex B contains a more detailed overview of the steps in the *risk management process*.

Compliance is checked by inspection of the appropriate documents.

© ISO 2019 – All rights reserved

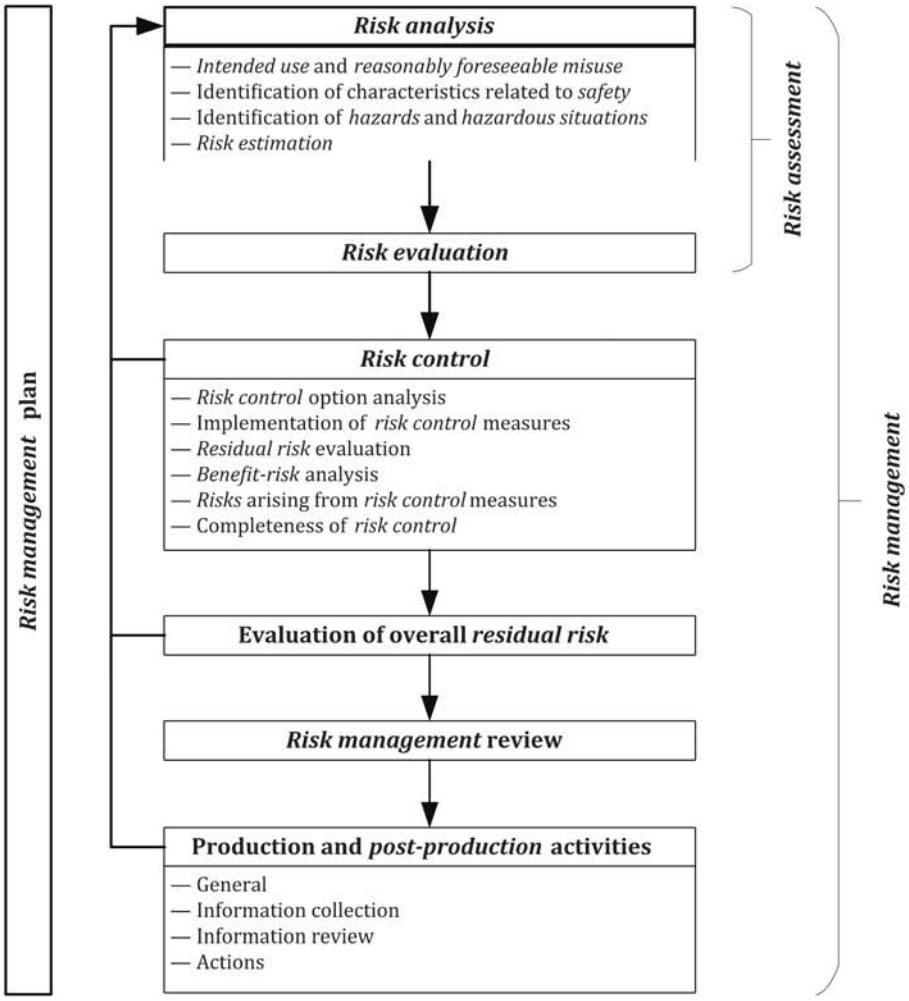


Figure 1 — A schematic representation of the *risk management process*

4.2 Management responsibilities

Top management shall provide evidence of its commitment to the *risk management process* by ensuring:

— the provision of adequate resources; and

— the assignment of competent personnel (see 4.3) for *risk management*.

Top management shall define and document a policy for establishing criteria for *risk* acceptability. The policy shall provide a framework that ensures that criteria are based upon applicable national or regional regulations and relevant International Standards, and take into account available information such as the generally acknowledged *state of the art* and known stakeholder concerns.

NOTE 1 The *manufacturer's* policy for establishing criteria for *risk* acceptability can define the approaches to *risk control*: reducing *risk* as low as reasonably practicable, reducing *risk* as low as reasonably achievable, or reducing *risk* as far as possible without adversely affecting the *benefit-risk* ratio. See ISO/TR 24971[9] for guidance on defining such policy.

Top management shall review the suitability of the *risk management process* at planned intervals to ensure continuing effectiveness of the *risk management process* and shall document any decisions and actions taken. If the *manufacturer* has a quality management system in place, this review may be part of the quality management system review.

NOTE 2 The results of reviewing production and *post-production* information can be an input to the review of the suitability of the *risk management process*.

© ISO 2019 – All rights reserved

NOTE 3 The documents described in this subclause can be incorporated within the documents produced by the *manufacturer's* quality management system and these documents can be referenced in the *risk management file*.

Compliance is checked by inspection of the appropriate documents.

4.3 Competence of personnel

Persons performing *risk management* tasks shall be competent on the basis of education, training, skills and experience appropriate to the tasks assigned to them. Where appropriate, these persons shall have knowledge of and experience with the particular *medical device* (or similar *medical devices*) and its use, the technologies involved or the *risk management* techniques employed. Appropriate *records* shall be maintained.

NOTE *Risk management* tasks can be performed by representatives of several functions, each contributing their specialist knowledge.

Compliance is checked by inspection of the appropriate *records*.

4.4 *Risk management* plan

Risk management activities shall be planned. For the particular *medical device* being considered, the *manufacturer* shall establish and document a *risk management* plan in accordance with the *risk management process*. The *risk management* plan shall be part of the *risk management file*.

This plan shall include at least the following:

a) the scope of the planned *risk management* activities, identifying and describing the *medical device* and the *life cycle* phases for which each element of the plan is applicable;

b) assignment of responsibilities and authorities;

c) requirements for review of *risk management* activities;

d) criteria for *risk* acceptability, based on the *manufacturer's* policy for determining acceptable *risk*, including criteria for accepting *risks* when the probability of occurrence of *harm* cannot be estimated;

NOTE 1 The criteria for *risk* acceptability are essential for the ultimate effectiveness of the *risk management process*. For each *risk management* plan the *manufacturer* needs to establish *risk* acceptability criteria that are appropriate for the particular *medical device*.

e) a method to evaluate the overall *residual risk*, and criteria for acceptability of the overall *residual risk* based on the *manufacturer's* policy for determining acceptable *risk*;

NOTE 2 The method to evaluate the overall *residual risk* can include gathering and reviewing data and literature for the *medical device* being considered and similar *medical devices* on the market and can involve judgment by a cross-functional team of experts with application knowledge and clinical expertise.

f) activities for *verification* of the implementation and effectiveness of *risk control* measures; and

g) activities related to collection and review of relevant production and *post-production* information.

NOTE 3 See ISO/TR 24971[9] for guidance on developing a *risk management* plan and on establishing criteria for *risk* acceptability.

NOTE 4 Not all parts of the plan need to be created at the same time. The plan or parts of it can be developed over time.

If the plan changes during the *life cycle* of the *medical device*, a *record* of the changes shall be maintained in the *risk management file*.

Compliance is checked by inspection of the *risk management file*.

© ISO 2019 – All rights reserved

4.5 *Risk management file*

For the particular *medical device* being considered, the *manufacturer* shall establish and maintain a *risk management file*. In addition to the requirements of other clauses of this document, the *risk management file* shall provide traceability for each identified *hazard* to:

— the *risk analysis*;

— the *risk evaluation*;

— the implementation and *verification* of the *risk control* measures; and

— the results of the evaluation of the *residual risks*.

NOTE 1 The *records* and other documents that make up the *risk management file* can form part of other documents and files required, for example, by a *manufacturer's* quality management system. The *risk management file* need not physically contain all the *records* and other documents. However, it needs to contain at least references or pointers to all required documentation, so that the *manufacturer* can assemble the information referenced in the *risk management file* in a timely manner.

NOTE 2 The *risk management file* can be in any form or type of medium.

NOTE 3 See ISO/TR 24971[9] for guidance on establishing a *risk management file* for components and devices that were designed without using ISO 14971.

5 *Risk analysis*

5.1 *Risk analysis process*

The *manufacturer* shall perform *risk analysis* for the particular *medical device* as described in 5.2 to 5.5. The implementation of the planned *risk analysis* activities and the results of the *risk analysis* shall be recorded in the *risk management file*.

NOTE 1 If a *risk analysis* or other relevant information is available for a similar *medical device*, that analysis or information can be used as a starting point for the new *risk analysis*. The degree of relevance depends on the differences between the *medical devices* and whether these introduce new *hazards* or significant differences in outputs, characteristics, performance or results. The extent of use of an existing *risk analysis* is based on a systematic evaluation of the effects that the differences can have on the occurrence of *hazardous situations*.

NOTE 2 See ISO/TR 24971[9] for guidance on selected *risk analysis* techniques and on *risk analysis* techniques for *in vitro diagnostic medical devices*.

In addition to the *records* required in 5.2 to 5.5, the documentation of the conduct and results of the *risk analysis* shall include at least the following:

a) identification and description of the *medical device* that was analysed;

b) identification of the person(s) and organization who carried out the *risk analysis*; and

c) scope and date of the *risk analysis*.

NOTE 3 The scope of the *risk analysis* can be very broad (as for the development of a new *medical device* with which a *manufacturer* has little or no experience) or the scope can be limited (as for analysing the impact of a change to an existing *medical device* for which much information already exists in the *manufacturer's* files).

Compliance is checked by inspection of the *risk management file*.

5.2 *Intended use* and *reasonably foreseeable misuse*

The *manufacturer* shall document the *intended use* of the particular *medical device* being considered.

 © ISO 2019 – All rights reserved

The *intended use* should take into account information such as the intended medical indication, patient population, part of the body or type of tissue interacted with, user profile, use environment, and operating principle.

The *manufacturer* shall also document *reasonably foreseeable misuse*.

This documentation shall be maintained in the *risk management file*.

NOTE 1 The use specification (see 3.23 of IEC 62366-1:2015[13]) can be an input to determining the *intended use*.

NOTE 2 See ISO/TR 24971[9] for factors to consider in determining the *intended use* and for an explanation of *reasonably foreseeable misuse*.

Compliance is checked by inspection of the *risk management file*.

5.3 Identification of characteristics related to *safety*

For the particular *medical device* being considered, the *manufacturer* shall identify and document those qualitative and quantitative characteristics that could affect the *safety* of the *medical device*. Where appropriate, the *manufacturer* shall define limits of those characteristics. This documentation shall be maintained in the *risk management file*.

NOTE 1 See ISO/TR 24971[9] for a list of questions that can serve as a guide in identifying *medical device* characteristics that could have an impact on *safety*.

NOTE 2 Characteristics related to loss or degradation of the clinical performance of a *medical device* that can result in unacceptable *risk*, are sometimes referred to as essential performance (see for example IEC 60601-1[12]).

Compliance is checked by inspection of the *risk management file*.

5.4 Identification of *hazards* and *hazardous situations*

The *manufacturer* shall identify and document known and foreseeable *hazards* associated with the *medical device* based on the *intended use*, *reasonably foreseeable misuse* and the characteristics related to *safety* in both normal and fault conditions.

For each identified *hazard*, the *manufacturer* shall consider the reasonably foreseeable sequences or combinations of events that can result in a *hazardous situation*, and shall identify and document the resulting *hazardous situation(s)*.

NOTE 1 A sequence of events can be initiated in all phases of the *life cycle*, e.g. during transport, storage, installation, maintenance, routine inspection, decommissioning and disposal.

NOTE 2 An explanation of the relationship between *hazard*, *hazardous situation* and *harm* including examples is given in Annex C.

NOTE 3 *Risk analysis* includes the examination of different sequences or combinations of events related to a single *hazard* that can lead to different *hazardous situations*. Each *hazardous situation* can lead to different types of *harm*.

NOTE 4 When identifying *hazardous situations* not previously recognised, systematic techniques for *risk analysis* that cover the specific situation can be used. Guidance on some available techniques is provided in ISO/TR 24971[9].

The documentation shall be maintained in the *risk management file*.

Compliance is checked by inspection of the *risk management file*.

5.5 *Risk estimation*

For each identified *hazardous situation*, the *manufacturer* shall estimate the associated *risk(s)* using available information or data. For *hazardous situations* for which the probability of the occurrence of

© ISO 2019 – All rights reserved

harm cannot be estimated, the possible consequences shall be listed for use in *risk evaluation* and *risk control*. The results of these activities shall be recorded in the *risk management file*.

The system used for qualitative or quantitative categorization of probability of occurrence of *harm* and *severity* of *harm* shall be recorded in the *risk management file*.

NOTE 1 *Risk estimation* incorporates an analysis of the probability of occurrence of *harm* and the *severity* of the *harm*. Depending on the area of application, only certain elements of the *risk estimation process* might need to be considered in detail. For example, when the *harm* is minimal, an initial *hazard* and consequence analysis could be sufficient, or when insufficient information or data are available, a conservative estimate of the probability of occurrence can give some indication of the *risk*. See also ISO/TR 24971[9].

NOTE 2 *Risk estimation* can be qualitative or quantitative. Methods of *risk estimation*, including those resulting from systematic faults, are described in ISO/TR 24971[9], which also gives information useful for estimating *risks* for *in vitro diagnostic medical devices*.

NOTE 3 Information or data for estimating *risks* can be obtained, for example, from:

— published standards;

— scientific or technical investigations;

— field data from similar *medical devices* already in use, including publicly available reports of incidents;

— usability tests employing typical users;

— clinical evidence;

— results of relevant investigations or simulations;

— expert opinion; or

— external quality assessment schemes for *in vitro diagnostic medical devices*.

Compliance is checked by inspection of the *risk management file*.

6 *Risk evaluation*

For each identified *hazardous situation*, the *manufacturer* shall evaluate the estimated *risks* and determine if the *risk* is acceptable or not, using the criteria for *risk* acceptability defined in the *risk management* plan.

If the *risk* is acceptable, it is not required to apply the requirements given in 7.1 to 7.5 to this *hazardous situation* (i.e., proceed to 7.6) and the estimated *risk* shall be treated as *residual risk*.

If the *risk* is not acceptable, then the *manufacturer* shall perform *risk control* activities as described in 7.1 to 7.6.

The results of this *risk evaluation* shall be recorded in the *risk management file*.

Compliance is checked by inspection of the *risk management file*.

7 *Risk control*

7.1 *Risk control* option analysis

The *manufacturer* shall determine *risk control* measures that are appropriate for reducing the *risks* to an acceptable level.

The *manufacturer* shall use one or more of the following *risk control* options in the priority order listed:

a) inherently safe design and manufacture;

© ISO 2019 – All rights reserved

b) protective measures in the *medical device* itself or in the manufacturing *process*;

c) information for *safety* and, where appropriate, training to users.

NOTE 1 The rationale for the priority order in selecting the *risk control* options is given in A.2.7.1.

NOTE 2 *Risk control* measures can reduce the *severity* of the *harm* or reduce the probability of occurrence of the *harm*, or both.

NOTE 3 See ISO/TR 24971[9] for guidance on providing information for *safety*.

Relevant standards should be applied as part of the *risk control* option analysis.

NOTE 4 Many standards address inherent *safety*, protective measures, and information for *safety* for *medical devices*. In addition, some *medical device* standards have integrated elements of the *risk management process* (e.g. electromagnetic compatibility, usability, biological evaluation). See ISO/TR 24971[9] for information on the role of International Standards in *risk management*.

The *risk control* measures selected shall be recorded in the *risk management file*.

If, during *risk control* option analysis, the *manufacturer* determines that *risk* reduction is not practicable, the *manufacturer* shall conduct a *benefit-risk* analysis of the *residual risk* (proceed to 7.4).

Compliance is checked by inspection of the *risk management file*.

7.2 Implementation of *risk control* measures

The *manufacturer* shall implement the *risk control* measures selected in 7.1.

Implementation of each *risk control* measure shall be verified. This *verification* shall be recorded in the *risk management file*.

NOTE 1 *Verification* of implementation can be performed as part of design and development *verification* or *process* qualification within a quality management system.

The effectiveness of the *risk control* measures shall be verified. The results of this *verification* shall be recorded in the *risk management file*.

NOTE 2 *Verification* of effectiveness can be performed as part of design and development validation within a quality management system and can include testing with users. See A.2.7.2.

NOTE 3 *Verification* of effectiveness can also be performed as part of design and development *verification* or *process* qualification, if the relationship between the effectiveness in *risk* reduction and the result of design and development *verification* or *process* qualification is known.

EXAMPLE 1 Design *verification* of a certain performance characteristic, such as dose accuracy of a drug injector, can serve as *verification* of effectiveness of *risk control* measures ensuring safe drug dosing.

EXAMPLE 2 *Process* qualification can serve as *verification* of effectiveness of *risk control* measures related to *risk* caused by variations in production output.

NOTE 4 See ISO 13485[5] for more information on design and development *verification* and validation. See also ISO/TR 24971[9] for more guidance.

Compliance is checked by inspection of the *risk management file*.

7.3 *Residual risk* evaluation

After the *risk control* measures are implemented, the *manufacturer* shall evaluate the *residual risk* using the criteria for *risk* acceptability defined in the *risk management* plan. The results of this evaluation shall be recorded in the *risk management file*.

If a *residual risk* is not judged acceptable using these criteria, further *risk control* measures shall be considered (go back to 7.1).

© ISO 2019 – All rights reserved

Compliance is checked by inspection of the *risk management file*.

7.4 *Benefit-risk* analysis

If a *residual risk* is not judged acceptable using the criteria established in the *risk management* plan and further *risk control* is not practicable, the *manufacturer* may gather and review data and literature to determine if the *benefits* of the *intended use* outweigh this *residual risk*.

If this evidence does not support the conclusion that the *benefits* outweigh this *residual risk*, then the *manufacturer* may consider modifying the *medical device* or its *intended use* (go back to 5.2). Otherwise, this *risk* remains unacceptable.

If the *benefits* outweigh the *residual risk*, then proceed to 7.5.

The results of the *benefit-risk* analysis shall be recorded in the *risk management file*.

NOTE See ISO/TR 24971[9] for guidance on performing a *benefit-risk* analysis.

Compliance is checked by inspection of the *risk management file*.

7.5 *Risks* arising from *risk control* measures

The *manufacturer* shall review the effects of the *risk control* measures with regard to whether:

— new *hazards* or *hazardous situations* are introduced; or

— the estimated *risks* for previously identified *hazardous situations* are affected by the introduction of the *risk control* measures.

Any new or increased *risks* shall be managed in accordance with 5.5 to 7.4.

The results of this review shall be recorded in the *risk management file*.

Compliance is checked by inspection of the *risk management file*.

7.6 Completeness of *risk control*

The *manufacturer* shall review the *risk control* activities to ensure that the *risks* from all identified *hazardous situations* have been considered and all *risk control* activities are completed.

The results of this review shall be recorded in the *risk management file*.

Compliance is checked by inspection of the *risk management file*.

8 Evaluation of overall *residual risk*

After all *risk control* measures have been implemented and verified, the *manufacturer* shall evaluate the overall *residual risk* posed by the *medical device*, taking into account the contributions of all *residual risks*, in relation to the *benefits* of the *intended use*, using the method and the criteria for acceptability of the overall *residual risk* defined in the *risk management* plan [see 4.4 e)].

If the overall *residual risk* is judged acceptable, the *manufacturer* shall inform users of significant *residual risks* and shall include the necessary information in the *accompanying documentation* in order to disclose those *residual risks*.

NOTE 1 The rationale for the disclosure of significant *residual risks* is given in A.2.8.

NOTE 2 See ISO/TR 24971[9] for guidance on the evaluation of overall *residual risk* and the disclosure of *residual risks*.

© ISO 2019 – All rights reserved

If the overall *residual risk* is not judged acceptable in relation to the *benefits* of the *intended use*, the *manufacturer* may consider implementing additional *risk control* measures (go back to 7.1) or modifying the *medical device* or its *intended use* (go back to 5.2). Otherwise, the overall *residual risk* remains unacceptable.

The results of the evaluation of the overall *residual risk* shall be recorded in the *risk management file*.

Compliance is checked by inspection of the *risk management file* and the *accompanying documentation*.

9 *Risk management* review

Prior to release for commercial distribution of the *medical device*, the *manufacturer* shall review the execution of the *risk management* plan. This review shall at least ensure that:

— the *risk management* plan has been appropriately implemented;

— the overall *residual risk* is acceptable; and

— appropriate methods are in place to collect and review information in the production and *post-production* phases.

The results of this review shall be recorded and maintained as the *risk management* report and shall be included in the *risk management file*.

The responsibility for review shall be assigned in the *risk management* plan to persons having the appropriate authority [see 4.4 b)].

Compliance is checked by inspection of the *risk management file*.

10 Production and *post-production* activities

10.1 General

The *manufacturer* shall establish, document and maintain a system to actively collect and review information relevant to the *medical device* in the production and *post-production* phases. When establishing this system, the *manufacturer* shall consider appropriate methods for the collection and processing of information.

NOTE 1 See also 7.3.3, 8.2.1, 8.4 and 8.5 of ISO 13485:2016[5].

NOTE 2 See ISO/TR 24971[9] for guidance on production and *post-production* activities.

Compliance is checked by inspection of the appropriate documents.

10.2 Information collection

The *manufacturer* shall collect, where applicable:

a) information generated during production and monitoring of the production *process*;

b) information generated by the user;

c) information generated by those accountable for the installation, use and maintenance of the *medical device*;

d) information generated by the supply chain;

e) publicly available information; and

f) information related to the generally acknowledged *state of the art*.

© ISO 2019 – All rights reserved

NOTE Information related to the generally acknowledged *state of the art* can include new or revised standards, published validated data specific to the application of the *medical device* under consideration, the availability of alternative *medical devices* and/or therapies, and other information (see also ISO/TR 24971[9]).

The *manufacturer* shall also consider the need to actively collect and review publicly available information about similar *medical devices* and similar other products on the market.

Compliance is checked by inspection of the appropriate documents.

10.3 Information review

The *manufacturer* shall review the information collected for possible relevance to *safety*, especially whether:

— previously unrecognised *hazards* or *hazardous situations* are present;

— an estimated *risk* arising from a *hazardous situation* is no longer acceptable;

— the overall *residual risk* is no longer acceptable in relation to the *benefits* of the *intended use*; or

— the generally acknowledged *state of the art* has changed.

The results of the review shall be recorded in the *risk management file*.

Compliance is checked by inspection of the *risk management file*.

10.4 Actions

If the collected information is determined to be relevant to *safety*, the following actions apply.

1) Concerning the particular *medical device*,

   — the *manufacturer* shall review the *risk management file* and determine if reassessment of *risks* and/or assessment of new *risks* is necessary;

   — if a *residual risk* is no longer acceptable, the impact on previously implemented *risk control* measures shall be evaluated and should be considered as an input for modification of the *medical device*;

   — the *manufacturer* should consider the need for actions regarding *medical devices* on the market; and

   — any decisions and actions shall be recorded in the *risk management file*.

2) Concerning the *risk management process*,

   — the *manufacturer* shall evaluate the impact on previously implemented *risk management* activities; and

   — the results of this evaluation shall be considered as an input for the review of the suitability of the *risk management process* by *top management* (see 4.2).

NOTE Some aspects of *post-production* monitoring are the subject of some national regulations. In such cases, additional measures might be required (e.g. prospective *post-production* evaluations).

Compliance is checked by inspection of the *risk management file* and other appropriate documents.

© ISO 2019 – All rights reserved

Annex A
(informative)

Rationale for requirements

A.1 General

The ISO/TC 210 — IEC/SC 62A Joint Working Group 1 (JWG 1), *Application of risk management to medical devices*, developed this rationale to document its reasoning for establishing the various requirements contained in this document. Those who make future revisions can use this annex, along with experience gained in the use of this document, to make this document more useful to *manufacturers*, regulatory bodies and health care providers.

ISO Technical Committee 210 and IEC Subcommittee 62A decided to combine their efforts on *risk management* and to form JWG 1 with the task to develop a standard for the application of *risk management* to *medical devices*. When discussions on an International Standard for *risk management* began, crucial features of *risk management* needed to be addressed, such as the *process* of *risk evaluation* as well as the balancing of *risks* and *benefits* for *medical devices*. *Manufacturers*, regulatory bodies, and health care providers had recognised that "absolute *safety*" in *medical devices* was not achievable. In addition, the *risks* that derive from the increasing diversity of *medical devices* and their applications cannot be completely addressed through product *safety* standards. The recognition of these facts and the consequent need to manage *risks* from *medical devices* throughout their *life cycle* led to the decision to develop ISO 14971 as a tool to actively improve the *safety* of *medical devices*. The first edition of this standard was published in 2000.

The second edition of ISO 14971 was developed and published in 2007 to address the need for additional guidance on its application and on the relationship between *hazards* and *hazardous situations*. Minor changes were made to the normative section, such as the addition of the requirement to plan for *post-production* monitoring and the removal of the requirement for traceability from the *risk management* report.

The systematic review in 2010 revealed the need for further guidance on a few specific topics. It was decided to develop the technical report ISO/TR 24971[9], because even a small update of the guidance would necessitate a revision of the standard. The first edition of this report was published in 2013.

This third edition was developed to clarify the normative requirements and to describe them in more detail, in particular the clauses on the evaluation of overall *residual risk*, on the *risk management* review and report and on production and *post-production* information. The clarifications were deemed necessary in view of requests for explanation in the systematic review of ISO 14971 in 2016 and in view of stricter requirements from regulatory bodies. More emphasis was put on the *benefits* that are anticipated from the use of the *medical device* and the balance between the (overall) *residual risks* and those *benefits*. It was explained that the *process* described in ISO 14971 can be applied to all types of *hazards* and *risks* associated with a *medical device*, for example biocompatibility, data and systems security, electricity, moving parts, radiation or usability. Several informative annexes were moved from this document to the guidance in ISO/TR 24971, which was revised in parallel. This allows for more frequent updates of the guidance independent of revising the standard.

A.2 Rationale for requirements in particular clauses and subclauses

A.2.1 Scope

As explained in the introduction to this document, a *risk management* standard applying to the *life cycle* of *medical devices* is required. Software as a *medical device* and *in vitro diagnostic medical devices* are

© ISO 2019 – All rights reserved

specifically mentioned in the scope to avoid any misunderstanding that, due to different regulations, these devices might be excluded from this document.

Risks can be present throughout the *life cycle* of the *medical device*, and *risks* that become apparent at one point in the *life cycle* can be managed by action taken at a completely different point in the *life cycle*. For this reason, the standard needs to be a complete *life cycle* standard. This means that the standard instructs *manufacturers* to apply *risk management* principles to a *medical device* from its initial conception until its ultimate decommissioning and disposal.

The *process* described in ISO 14971 can be applied to *hazards* and *risks* associated with the *medical device*. *Risks* related to data and systems security are specifically mentioned in the scope, to avoid any misunderstanding that a separate *process* would be needed to manage security *risks* related to *medical devices*. This does not preclude the possibility of developing specific standards, in which specific methods and requirements are provided for the assessment and control of security *risks*. Such standards can be used in conjunction with ISO 14971, in a similar way as IEC 62366-1[13] for usability, ISO 10993-1[4] for biological evaluation, or IEC 60601-1[12] for electrical and mechanical *risks*.

The scope of this document does not include clinical decision making, i.e., decisions on the use of a *medical device* in the context of a particular clinical *procedure*. Such decisions require the *residual risks* to be balanced against the anticipated *benefits* of the *procedure* or the *risks* and anticipated *benefits* of alternative *procedures*. Such decisions take into account the *intended use*, performance and *risks* associated with the *medical device* as well as the *risks* and *benefits* associated with the clinical *procedure* or the circumstances of use. Some of these decisions can be made only by a qualified health care professional with knowledge of the state of health of an individual patient and the patient's own opinion.

The scope of this document also does not include business decision making. Other standards such as ISO 31000[10] exist for organisational *risk management* and related topics.

Although there has been significant debate over what constitutes an acceptable level of *risk*, this document does not specify acceptability levels. Specifying a universal level for acceptable *risk* could be inappropriate. This decision is based upon the belief that:

— the wide variety of *medical devices* and situations covered by this document would make a universal level for acceptable *risk* meaningless;

— local laws, customs, values and perception of *risk* are more appropriate for defining *risk* acceptability for a particular culture or region of the world.

Because not all countries require a quality management system for *medical device manufacturers*, a quality management system is not a requirement of this document. However, a quality management system is extremely helpful in managing *risks* properly. Because of this and because most *medical device manufacturers* do employ a quality management system, this document is constructed so that it can easily be incorporated into the quality management system that they use.

A.2.2 Normative references

No other standards are required in order to establish and maintain a *risk management process* in accordance with ISO 14971. Clause 15 of ISO/IEC Directives, Part 2:2018, requires standards to include this statement.

A.2.3 Terms and definitions

Most of the definitions used in this document are taken from ISO 9000:2015[3] and ISO/IEC Guide 63:2019[2] which in turn adopted and adapted many of the definitions in ISO/IEC Guide 51:2014[1] and the definitions developed by the Global Harmonization Task Force (GHTF). Some of these definitions have a slightly different meaning in ISO/IEC Guide 63:2019[2] and ISO 14971 than in other standards.

For example, JWG 1 intended the definition of *harm* (3.3) to have a broad range and to include unreasonable psychological stress or unwanted pregnancy as part of "damage to the health of

© ISO 2019 – All rights reserved

people". Such stress can occur after a false positive diagnosis of a disease. "Damage to property and the environment" is undesirable and the associated *risks* need to be considered as well, for example those related to hazardous waste materials created by the use or disposal of the *medical device*. The word "physical" is removed from the definition of *harm* in ISO/IEC Guide 51:2014[1] and thus also in ISO/IEC Guide 63:2019 [2] and this document, because injury by itself already includes physical damage. Breaches of data and systems security can lead to *harm*, e.g. through loss of data, uncontrolled access to data, corruption or loss of diagnostic information, or corruption of software leading to malfunction of the *medical device*.

The definition of the term *intended use* (3.6) combines the definition of *intended use* as used in the United States and *intended purpose* which is the term in the European Union. These terms have essentially the same definition. It was intended that, when determining the *intended use* of a *medical device*, the *manufacturer* takes into account the intended medical indication, patient population, part of the body or tissue interacted with, user profile, use environment, and operating principle. The definition of *life cycle* (3.8) was necessary to make it clear that the term as used in this document covers all aspects of the existence of a *medical device*. The definition for *risk management* (3.24) emphasises the use of a systematic approach and the need for management oversight. The definition of *top management* (3.29) uses the definition from ISO 9000:2015[3]. It applies to the person or group at the highest level in the *manufacturer's* organization.

Three other terms in ISO 14971 are not based on definitions in ISO/IEC Guide 63:2019[2] or in other standards. They are *benefit* (3.2), *post-production* (3.12) and *risk management file* (3.25). The term *benefit* is defined because of the increased emphasis by regulatory bodies on balancing the (*residual*) *risks* against the *benefits* of the *medical device*. For the same reason the phrase "*benefit-risk* analysis" is used. A definition of *post-production* was added to emphasise that the entire *life cycle* of the *medical device* is important for *risk management*. The concept of a *risk management file* is now well understood.

A.2.4 General requirements for *risk management* system

A.2.4.1 *Risk management process*

The *risk management* system consists of the elements in 4.1 through 4.5.

The *manufacturer* needs to establish a *risk management process* as part of the design and development of a *medical device*. This is required so that the *manufacturer* can systematically ensure that the required elements are in the *process*. *Risk analysis*, *risk evaluation* and *risk control* are commonly recognised as essential parts of *risk management*. In addition to these elements, this document emphasises that the *risk management process* does not end with the design and production (including, as relevant, sterilization, packaging, and labelling) of a *medical device*, but continues on into the *post-production* phase. Therefore, the collection and review of production and *post-production* information was identified as a required part of the *risk management process*. Furthermore, it was felt that when a *manufacturer* employs a quality management system, the *risk management process* should be fully integrated into that quality management system.

Although *risk management* activities are highly individual to the *medical device* being considered, there are basic elements that need to be included in the *risk management process*. This need is addressed in 4.1. This subclause also recognises that there can be some differences in regulatory approaches to applying *risk management* to *medical devices*.

Subclauses 4.2 and 4.3 closely follow the *risk*-related requirements of quality management system standards. In some countries a quality management system is always required to market a *medical device* (unless the *medical device* is specifically exempted). In other countries *manufacturers* can choose whether to apply a quality management system. However, the requirements of 4.2 and 4.3 are always needed for an effective *risk management process*, whether or not the *manufacturer* operates all the other elements of a quality management system.

© ISO 2019 – All rights reserved

A.2.4.2 Management responsibilities

The commitment of *top management* is critical for an effective *risk management process*. These individuals are responsible for overall guidance of the *risk management process* and this subclause is intended to emphasise their role. In particular:

— in the absence of adequate resources, *risk management* activities would be less effective, even if complying, to the letter, with the other requirements of this document;

— *risk management* is a specialized discipline and requires the involvement of competent individuals trained in *risk management* techniques (see A.2.4.3);

— because this document does not define acceptable *risk* levels, *top management* is required to establish a policy on how acceptable *risks* will be determined;

— *risk management* is an evolving *process* and periodic review of the *risk management* activities is needed to ascertain whether they are being carried out correctly, to rectify any weaknesses, to implement improvements, and to adapt to changes.

A.2.4.3 Competence of personnel

It is most important to get competent people with the knowledge and experience necessary to perform *risk management* tasks. The *risk management process* requires people with knowledge and experience in areas such as:

— how the *medical device* is constructed;

— how the *medical device* works;

— how the *medical device* is produced;

— how the *medical device* is actually used;

— how to apply the *risk management process*.

In general, this usually requires several representatives from various functions or disciplines, each contributing their specialist knowledge. The balance and relation between those representatives should be considered.

Records are required to provide *objective evidence* of competence. In order to avoid duplication and because of confidentiality and data protection considerations, this document does not require these *records* to be kept in the *risk management file*.

A.2.4.4 *Risk management* plan

A *risk management* plan is required because:

— an organized approach is essential for good *risk management*;

— the plan provides the roadmap for *risk management*;

— the plan encourages objectivity and helps prevent essential elements being forgotten.

The elements a) to g) of 4.4 are required for the following reasons.

a) There are two distinct elements in the scope of the plan. The first identifies the *medical device*, the other identifies the phase of the *life cycle* for which each element of the plan is applicable. By defining the scope, the *manufacturer* establishes the baseline on which all the *risk management* activities are built.

b) Allocation of responsibilities and authorities is needed to ensure that no responsibility is omitted.

© ISO 2019 – All rights reserved

c) Review of activities such as *risk management* is included as a generally recognised responsibility of management.

d) The criteria for *risk* acceptability are fundamental to *risk management* and should be decided upon before *risk analysis* begins. This helps to make the *risk evaluation* in Clause 6 objective.

e) After implementing all *risk control* measures, the *manufacturer* is required to evaluate the overall impact of all *residual risks* together. The evaluation method and the criteria for acceptability of the overall *residual risk* should be decided upon before this evaluation is performed. This helps to make the evaluation of overall *residual risk* in Clause 8 objective.

f) *Verification* is an essential activity and is required by 7.2. Planning this activity helps to ensure that essential resources are available when required. If *verification* is not planned, important parts of the *verification* could be neglected.

g) Methods for the collection and review of production and *post-production* information need to be established so that there is a formal and appropriate way to feed back production and *post-production* information into the *risk management process*.

The requirement to keep a *record* of changes is to facilitate audit and review of the *risk management process* for a particular *medical device*.

A.2.4.5 *Risk management file*

This document uses this term to signify where the *manufacturer* can locate or find the locations of all the *records* and other documents applicable to *risk management*. This facilitates the *risk management process* and enables more efficient auditing to this document. Traceability is necessary to demonstrate that the *risk management process* has been applied to each identified *hazard*.

Completeness is very important in *risk management*. An incomplete task can mean that an identified *hazard* is not controlled and *harm* can be the consequence. The problem can result from incompleteness at any step in *risk management*, e.g. unidentified *hazards*, *risks* not assessed, unspecified *risk control* measures, *risk control* measures not implemented, or *risk control* measures that prove ineffective. Traceability is needed to ensure completeness of the *risk management process*.

A.2.5 *Risk analysis*

A.2.5.1 *Risk analysis process*

Note 1 of 5.1 describes how to deal with the availability of a *risk analysis* for a similar *medical device*. When adequate information already exists, this information can be applied to save time, effort and resources. Users of this document need to be careful, however, to assess systematically the previous work for applicability to the current *risk analysis*.

The details required by a), b), and c) form the basic minimum data set for ensuring traceability and are important for management reviews and for subsequent audits. The requirement in c) also helps clarify what is in the scope of the analysis and verifies completeness.

A.2.5.2 *Intended use* and *reasonably foreseeable misuse*

The *intended use* of the *medical device* is an important aspect and is the starting point of the *risk analysis*. This should include the elements listed in the note to 3.6, where appropriate. The *manufacturer* should also consider the intended user(s) of the *medical device*, e.g., whether a lay user or a trained medical professional will use the *medical device*. This analysis should consider that *medical devices* can also be used in situations other than those intended by the *manufacturer* and in situations other than those foreseen when the idea for a *medical device* was first conceived. It is important that the *manufacturer* tries to look into the future to see the *hazards* due to potential uses of their *medical device* and also the *reasonably foreseeable misuse*.

© ISO 2019 – All rights reserved

A.2.5.3 Identification of characteristics related to *safety*

This step forces the *manufacturer* to think about all the characteristics that could affect the *safety* of the *medical device*. These characteristics can be qualitative or quantitative and can be related to the operating principle of the *medical device*, its *intended use* and/or the *reasonably foreseeable misuse*. Such characteristics can relate to the performance or operating principle of the *medical device*, the measuring function or the sterility of the *medical device*, the materials used for parts coming into contact with the patient, the use of radiation for diagnostic or therapeutic purposes, or other. Where applicable, the limits of those characteristics need to be considered as well, because the operation and/or *safety* of the *medical device* could be affected when those limits are exceeded.

A.2.5.4 Identification of *hazards* and *hazardous situations*

This step requires the *manufacturer* to be systematic in the identification of anticipated *hazards* in both normal and fault conditions. The identification should be based upon the *intended use* and *reasonably foreseeable misuse* identified in 5.2 and the characteristics related to *safety* identified in 5.3.

A *risk* can only be assessed and managed once a *hazardous situation* has been identified. Documenting the reasonably foreseeable sequences of events that can transform a *hazard* into a *hazardous situation* allows this to be done systematically. Annex C aims to assist *manufacturers* in identifying *hazards* and *hazardous situations*. Typical *hazards* are listed and the relationships between *hazards*, foreseeable sequences of events, *hazardous situations* and associated possible *harm* are demonstrated.

A.2.5.5 *Risk estimation*

This is the final step of *risk analysis*. The difficulty of this step is that *risk estimation* is different for every *hazardous situation* that is under investigation as well as for every *medical device*. Therefore, this subclause was written generically. Because *hazards* can occur both when the *medical device* functions normally and when it malfunctions, one should look closely at both situations. In practice, both components of *risk*, probability of occurrence and *severity* of *harm*, should be analysed separately. When a *manufacturer* uses a systematic way of categorizing the *severity* levels or the probability of occurrence of *harm*, the categorization scheme should be defined and recorded in the *risk management file*. This enables the *manufacturer* to treat equivalent *risks* consistently and serves as evidence that the *manufacturer* has done so.

Some *hazardous situations* occur because of systematic faults or sequences of events. There is no consensus on how to calculate the probability of a systematic fault. Where the probability of occurrence of *harm* cannot be calculated, *hazards* still have to be addressed and listing resulting *hazardous situations* separately allows the *manufacturer* to focus on reducing the *risks* due to these *hazardous situations*.

Frequently, good quantitative data are not readily available, especially in development of an entirely new *medical device* or for security *risks*. The suggestion that *risk estimation* should be done only in a quantitative way has therefore been avoided.

A.2.6 *Risk evaluation*

Decisions have to be made about the acceptability of *risk*. *Manufacturers* can use the estimated *risks* and evaluate them using the criteria for *risk* acceptability defined in the *risk management* plan. They can investigate the *risks* to determine which ones need to be controlled. Clause 6 was carefully worded to allow the user of this document to avoid unnecessary work.

A.2.7 *Risk control*

A.2.7.1 *Risk control* option analysis

Often there will be more than one way to reduce a *risk*. There are three mechanisms listed, which are all standard *risk* reduction measures and are derived from ISO/IEC Guide 63:2019[2]. The priority order listed is important. This principle is found in several places, including IEC TR 60513[11] and local or

© ISO 2019 – All rights reserved

regional regulations. Inherently safe design and manufacture is the first and most important option in the *risk control* option analysis, because design solutions inherent to the characteristics of the *medical device* are likely to remain effective, whereas experience has shown that even well-designed guards and protective measures can fail or be violated and information for *safety* might not be followed. If practicable, the *medical device* should be designed and manufactured to be inherently safe. If this is not practicable, then protective measures such as barriers or alarms are appropriate. The third option is to provide information for *safety* such as a written warning or contra-indication. Training to users can be an important aspect of delivering information for *safety*. The *manufacturer* can consider to provide mandatory training for the intended users.

The manufacturing *process* can contribute to *risks*, for example originating from contamination of components, residues of hazardous substances used in the *process*, or mix-up of parts. Such *risks* can be controlled by designing the manufacturing *process* to be inherently safe (e.g. eliminating hazardous substances or using separate production lines) or by applying protective measures (e.g. visual inspection steps in the *process*).

It is recognised that one possible result of the *risk control* option analysis could be that there is no practicable way of reducing the *risk* to acceptable levels according to the pre-established criteria for *risk* acceptability. For example, it could be impractical to design a life-supporting *medical device* with such an acceptable *residual risk*. In this case, a *benefit-risk* analysis can be carried out as described in 7.4 to determine whether the *benefit* of the *medical device*, to the patient, outweighs the *residual risk*. This option is included at this point in the document to make sure that every effort was first made to reduce *risks* to the pre-established acceptable levels.

A.2.7.2 Implementation of *risk control* measures

Two distinct *verifications* are included. The first *verification* is required to make sure that the *risk control* measure has been implemented in the final design of the *medical device* or in the manufacturing *process*. The second *verification* is required to ensure that the *risk control* measure (including information for *safety*) as implemented actually reduces the *risk*. In some instances, a validation study can be used for verifying the effectiveness of the *risk control* measure.

Obtaining sufficient data and information for *risk estimation* can be difficult, resulting in uncertainty of the *residual risk* evaluation. It can therefore be practical for the *manufacturer* to focus effort on *verification* of effectiveness of *risk control* measures to establish a convincing *residual risk* evaluation. Level of effort should be commensurate with the level of *risk*. Testing with users might be needed to verify the effectiveness of the *risk controls*, for example usability testing (see IEC 62366-1[13]), clinical investigation of *medical devices* (see ISO 14155[1)][6]) or clinical performance studies for *in vitro diagnostic medical devices* (see ISO 20916[8]). A usability test can verify effectiveness of information for *safety* and a test according to a test standard can verify effectiveness of designed *risk control* measures related to, for example, mechanical strength.

A.2.7.3 *Residual risk* evaluation

A check was introduced here to determine whether the implemented *risk control* measures have made the *risk* acceptable. If the *risk* exceeds the acceptability criteria established in the *risk management* plan, the *manufacturer* is instructed to investigate additional *risk control* measures. This iterative *procedure* should be continued until further *risk control* is not practicable and the *residual risk* does not exceed the acceptability criteria established in the *risk management* plan.

A.2.7.4 *Benefit-risk* analysis

There can be particular *hazardous situations* for which the *risk* exceeds the *manufacturer's* criteria for *risk* acceptability. This subclause enables the *manufacturer* to provide a high-*risk medical device* for which they have done a careful evaluation and can show that the *benefit* of the *medical device* outweighs the *risk*. However, this subclause cannot be used to weigh *residual risks* against economic advantages or business advantages (i.e. for business decision making).

1) Under preparation. Stage at the time of publication ISO/FDIS 14155:2019.

© ISO 2019 – All rights reserved

A.2.7.5 *Risks* arising from *risk control* measures

This subclause recognises that *risk control* measures alone or in combination might introduce a new and sometimes quite different *hazard*, and that *risk control* measures introduced to reduce one *risk* might increase another *risk*.

A.2.7.6 Completeness of *risk control*

At this point, the *risks* of all the *hazardous situations* should have been evaluated. This check was introduced to ensure that no *hazardous situations* were left out in the intricacies of a complex *risk analysis*.

A.2.8 Evaluation of overall *residual risk*

During the *process* defined by Clauses 5 to 7, *manufacturers* identify *hazards* and *hazardous situations*, evaluate the *risks*, and implement *risk control* measures in their *medical device* design one at a time. This is the point where the *manufacturer* has to step back, consider the combined impact of all individual *residual risks*, and make a decision as to whether to proceed with the *medical device*. It is possible that the overall *residual risk* exceeds the *manufacturer's* criteria for *risk* acceptability, even though individual *residual risks* do not. This is particularly true for complex systems and *medical devices* with a large number of *risks*. The method to evaluate the overall *residual risk* as defined in the *risk management* plan includes balancing the overall *residual risk* against the *benefits* of the *medical device*. This is particularly relevant in determining whether a high-*risk*, but highly beneficial, *medical device* should be marketed.

The *manufacturer* is responsible for providing users with relevant information on significant *residual risks*, so that they can make informed decisions on the use of the *medical device*. Thus, *manufacturers* are instructed to include pertinent information on *residual risks* in the *accompanying documentation*. However, it is the *manufacturer's* decision as to what and how much information should be provided. This requirement is consistent with the approach taken in many countries and regions.

A.2.9 *Risk management* review

The *risk management* review is an important step before the commercial release of the *medical device*. The final results of the *risk management process*, as obtained by executing the *risk management* plan, are reviewed. The *risk management* report contains the results of this review and is a crucial part of the *risk management file*. The report serves as the high-level document that provides evidence that the *manufacturer* has ensured that the *risk management* plan has been satisfactorily fulfilled and the results confirm that the required objective has been achieved. Subsequent reviews of the execution of the *risk management* plan and updates of the *risk management* report can be needed during the *life cycle* of the *medical device*, as a result of the execution of production and *post-production* activities.

A.2.10 Production and *post-production* activities

It cannot be emphasized too often that *risk management* does not stop when a *medical device* goes into production. *Risk management* often begins with an idea, before there is any physical manifestation of the *medical device*. *Manufacturers* collect information from many sources, including experience with similar *medical devices* and technologies. *Risk estimation* is refined throughout the design *process* and can be made more accurate when a functioning prototype is built. However, no amount of modelling can substitute for an actual *medical device* in the hands of actual users.

Therefore, the *manufacturer* needs to collect and review production and *post-production* information and evaluate its relevance to safety. The information can relate to new *hazards* or *hazardous situations*, and/or can affect their *risk* estimates or the balance between *benefit* and overall *residual risk*. Either can impact the *manufacturer's risk management* decisions. The *manufacturer* should also take into account considerations of the generally acknowledged *state of the art*, including new or revised standards. When the information is determined to be relevant to *safety*, the *risk management process* requires that it be considered as an input for modification of the *medical device*, and also as an input to improve the *process* itself. With effective production and *post-production* activities, the *risk management process* truly becomes an iterative closed-loop *process* to ensure the continued *safety* of the *medical device*.

© ISO 2019 – All rights reserved

In reply to feedback and requests for additional guidance and in response to changing regulatory requirements, the requirements for production and *post-production* activities are elaborated in more detail in this third edition. The clause is divided into subclauses. More sources of information are listed, including information on the generally acknowledged *state of the art* and feedback from the supply chain. The latter includes suppliers of components or subsystems, and also third-party software. The possible need for actions regarding *medical devices* already on the market is made more explicit. The conditions under which follow-up actions need to be considered, are extended with changes in the *state of the art* that can be relevant to *safety*, such as alternative *medical devices* and/or therapies becoming available on the market, as well as changes in *risk* perception or *risk* acceptability.

© ISO 2019 – All rights reserved

Annex B
(informative)

Risk management process for *medical devices*

B.1 Correspondence between second and third editions

The numbering of clauses and subclauses has changed with this third edition of ISO 14971. Table B.1 provides the correspondence between clauses and subclauses in the second edition ISO 14971:2007 and those in the third edition ISO 14971:2019. This table is provided to assist users of this document in transitioning from the second to the third edition and to facilitate updating of references to ISO 14971 in other documents.

Table B.1 — Correspondence between elements of ISO 14971:2007 and ISO 14971:2019

ISO 14971:2007	ISO 14971:2019
Introduction	Introduction
1 Scope	1 Scope
(New clause)	2 Normative references
2 Terms and definitions	3 Terms and definitions
2.1 *accompanying document*	3.1 *accompanying documentation*
(New definition)	3.2 *benefit*
2.2 *harm*	3.3 *harm*
2.3 hazard	3.4 *hazard*
2.4 hazardous situation	3.5 *hazardous situation*
2.5 intended use intended purpose	3.6 *intended use* *intended purpose*
2.6 in vitro diagnostic medical device IVD medical device	3.7 *in vitro diagnostic medical device* *IVD medical device*
2.7 life-cycle	3.8 *life cycle*
2.8 manufacturer	3.9 *manufacturer*
2.9 medical device	3.10 *medical device*
2.10 objective evidence	3.11 *objective evidence*
2.11 post-production	3.12 *post-production*
2.12 procedure	3.13 *procedure*
2.13 process	3.14 *process*
(New definition)	3.15 *reasonably foreseeable misuse*
2.14 record	3.16 *record*
2.15 residual risk	3.17 *residual risk*

© ISO 2019 – All rights reserved

Table B.1 *(continued)*

ISO 14971:2007	ISO 14971:2019
2.16 risk	3.18 *risk*
2.17 risk analysis	3.19 *risk analysis*
2.18 risk assessment	3.20 *risk assessment*
2.19 risk control	3.21 *risk control*
2.20 risk estimation	3.22 *risk estimation*
2.21 risk evaluation	3.23 *risk evaluation*
2.22 risk management	3.24 *risk management*
2.23 risk management file	3.25 *risk management file*
2.24 safety	3.26 *safety*
2.25 severity	3.27 *severity*
(New definition)	3.28 *state of the art*
2.26 top management	3.29 *top management*
2.27 use error	3.30 *use error*
2.28 verification	3.31 *verification*
3 General requirements for risk management	4 General requirements for *risk management* system
3.1 Risk management process	4.1 *Risk management process*
3.2 Management responsibilities	4.2 Management responsibilities
3.3 Qualification of personnel	4.3 Competence of personnel
3.4 Risk management plan	4.4 *Risk management* plan
3.5 Risk management file	4.5 *Risk management file*
4 Risk analysis	5 *Risk analysis*
4.1 Risk analysis process	5.1 *Risk analysis process*
4.2 Intended use and identification of characteristics related to the safety of the medical device	5.2 *Intended use* and *reasonably foreseeable misuse*
	5.3 Identification of characteristics related to *safety*
4.3 Identification of hazards	5.4 Identification of *hazards* and *hazardous situations*
4.4 Estimation of the risk(s) for each hazardous situation	5.5 *Risk estimation*
5 Risk evaluation	6 *Risk evaluation*
6 Risk control	7 *Risk control*
6.1 Risk reduction	(Subclause deleted)
6.2 Risk control option analysis	7.1 *Risk control* option analysis
6.3 Implementation of risk control measure(s)	7.2 Implementation of *risk control* measures
6.4 Residual risk evaluation	7.3 *Residual risk* evaluation
6.5 Risk/benefit analysis	7.4 *Benefit-risk* analysis
6.6 Risks arising from risk control measures	7.5 *Risks* arising from *risk control* measures
6.7 Completeness of risk control	7.6 Completeness of *risk control*
7 Evaluation of overall residual risk acceptability	8 Evaluation of overall *residual risk*
8 Risk management report	9 *Risk management* review

© ISO 2019 – All rights reserved

Table B.1 *(continued)*

ISO 14971:2007	ISO 14971:2019
9 Production and post-production information	10 Production and *post-production* activities
	10.1 General
	10.2 Information collection
	10.3 Information review
	10.4 Actions
Annex A Rationale for requirements	Annex A Rationale for requirements
Annex B Overview of the risk management process for medical devices	Annex B *Risk management process* for *medical devices*
Annex C Questions that can be used to identify medical device characteristics that could impact on safety	Moved to ISO/TR 24971
Annex D Risk concepts applied to medical devices	
Annex E Examples of hazards, foreseeable sequences of events and hazardous situations	Annex C Fundamental *risk* concepts
Annex F Risk management plan	Moved to ISO/TR 24971
Annex G Information on risk management techniques	
Annex H Guidance on risk management for in vitro diagnostic medical devices	
Annex I Guidance on risk analysis process for biological hazards	(Annex deleted)
Annex J Information for safety and information about residual risk	Moved to ISO/TR 24971
Bibliography	Bibliography

B.2 *Risk management process* overview

Figure B.1 is provided to give the user of this document an overview of the *risk management process*. It is for illustrative purposes only. As indicated in Figure B.1, the *process* needs to be iterative, covering each *risk* in turn, and returning to earlier steps if *risk control* measures introduce new *hazards* or *hazardous situations*, or if new information becomes available.

© ISO 2019 – All rights reserved

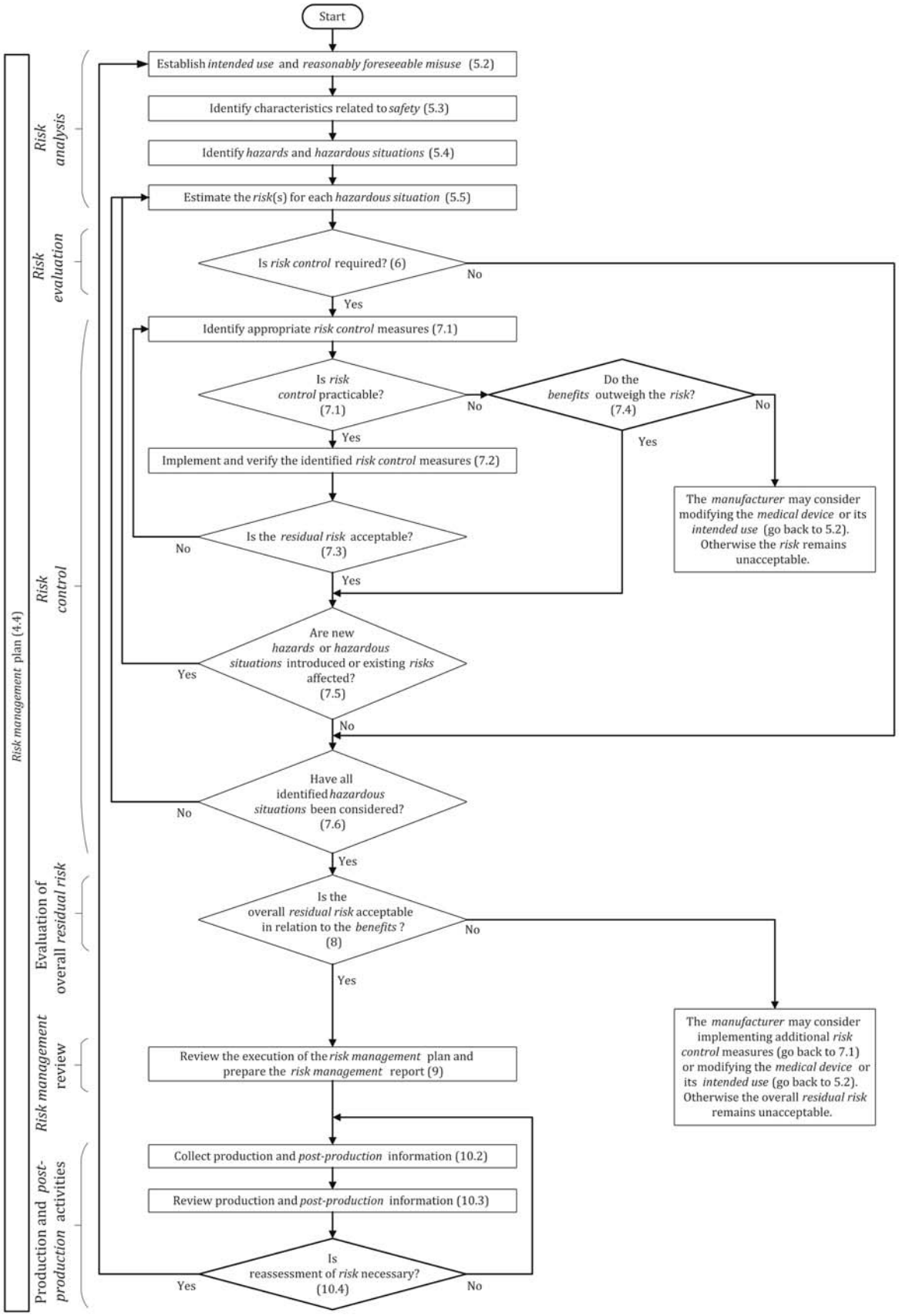


Figure B.1 — Overview of *risk management* activities as applied to *medical devices*

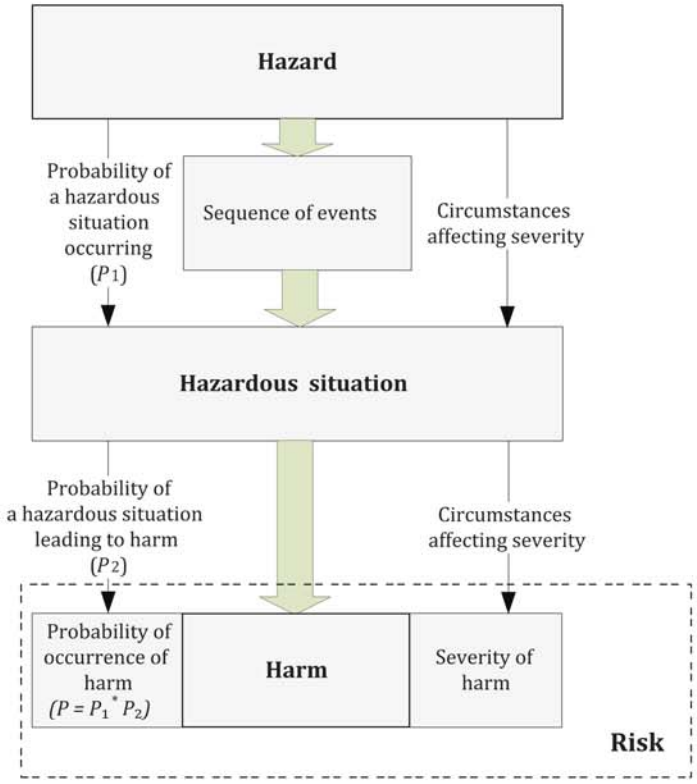
© ISO 2019 – All rights reserved

Annex C
(informative)

Fundamental *risk* concepts

C.1 General

This document requires the *manufacturer* to compile a list of known and foreseeable *hazards* associated with the *medical device* in both normal and fault conditions and to consider the foreseeable sequences of events that can produce *hazardous situations* and *harm*. According to the definitions, a *hazard* cannot result in *harm* until such time as a sequence of events or other circumstances (including normal use) lead to a *hazardous situation*. At this point, the *risk* can be assessed by estimating both *severity* and probability of occurrence of *harm* that could result (see Figure C.1). The probability of occurrence of *harm* can be expressed as a combination of separate probabilities (P_1, P_2) or as a single probability (P). A decomposition into P_1 and P_2 is not mandatory.



NOTE 1 Depending on the complexity of the *medical device*, a *hazard* can lead to multiple *hazardous situations*, and each *hazardous situation* can lead to multiple *harms*.

NOTE 2 The probability of occurrence of *harm* (P) can be composed of separate P_1 and P_2 values.

NOTE 3 The thin arrows represent elements of *risk analysis* and the thick arrows depict how a *hazard* can lead to *harm*

Figure C.1 — Pictorial example of the relationship between *hazard*, sequence of events, *hazardous situation* and *harm* (from ISO/IEC Guide 63:2019[2])

© ISO 2019 – All rights reserved

A good starting point for this compilation is a review of experience with the same and similar types of *medical devices*. The review should take into account a *manufacturer's* own experience and, where appropriate, the experience of other *manufacturers* as reported in adverse event databases, publications, scientific literature and other available sources. This type of review is particularly useful for the identification and listing of typical *hazards* and *hazardous situations* for a *medical device* and the associated *harm* that can occur. Next, this listing and aids such as the list of examples in Table C.1 can be used to compile an initial list of *hazards*.

It is then possible to begin identification of some of the sequences of events that together with *hazards* could result in *hazardous situations* and *harm*. Since many *hazards* might never result in *harm* and can be eliminated from further consideration, it could be useful to perform this analysis by starting with the *harm* that the *medical device* might cause and work backwards to the *hazardous situations*, *hazards* and initiating causes. However, although this approach is useful for the reason described, it should be recognised that it is not a thorough analysis. Many sequences of events will only be identified by the systematic use of *risk analysis* techniques (such as those described in ISO/TR 24971[9]). Analysis and identification are further complicated by the many events and circumstances that have to be taken into consideration such as those listed in Table C.2. Thus, more than one *risk analysis* technique, and especially complementary techniques, are often used to complete a comprehensive analysis. Table C.3 provides examples of the relationship between *hazards*, sequences of events, *hazardous situations*, and *harm*.

Although compilation of the lists of *hazards*, *hazardous situations* and sequences of events should be completed as early as possible in the design and development *process* to facilitate *risk control*, in practice identification and compilation is an ongoing activity that continues throughout the *life cycle* of the *medical device* through *post-production* to disposal.

This annex provides a non-exhaustive list of possible *hazards* that can be associated with different *medical devices* (Table C.1) and a list of events and circumstances (Table C.2) that can result in *hazardous situations*, which can result in *harm*. Table C.3 provides examples in a logical progression of how a *hazard* can be transformed into a *hazardous situation* and produce *harm* by a sequence of events or circumstances.

Recognising how *hazards* progress to *hazardous situations* is critical for estimating the probability of occurrence and *severity* of *harm* that could result. An objective of the *process* is to compile a comprehensive set of *hazardous situations*. The identification of *hazards* and sequences of events are stepping stones to achieve this. The lists in the tables in this annex can be used to aid in the identification of *hazardous situations*. What is called a *hazard* needs to be determined by the *manufacturer* to suit the particular analysis.

C.2 Examples of *hazards*

The list in Table C.1 can be used to assist in the identification of *hazards* associated with a particular *medical device*, which could ultimately result in *harm*.

© ISO 2019 – All rights reserved

Table C.1 — Examples of *hazards*

Energy *hazards*	Biological and chemical *hazards*	Performance-related *hazards*
Acoustic energy	**Biological agents**	**Data**
— infrasound	Bacteria	— access
— sound pressure	Fungi	— availability
— ultrasonic	Parasites	— confidentiality
Electric energy	Prions	— transfer
Electric fields	Toxins	— integrity
Leakage current	Viruses	**Delivery**
— earth leakage	**Chemical agents**	— quantity
— enclosure leakage	Carcinogenic, mutagenic, reproductive	— rate
Magnetic fields	Caustic, corrosive	**Diagnostic information**
Static discharge	— acidic	— examination result
Voltage	— alkaline	— image artefacts
Mechanical energy	— oxidants	— image orientation
Kinetic energy	Flammable, combustible, explosive	— image resolution
— falling objects	Fumes, vapors	— patient identity / information
— high pressure fluid injection	Osmotic	**Functionality**
— moving parts	Particles (including micro- and nano-particles)	— alarm
— vibrating parts	Pyrogenic	— critical performance
Potential (stored) energy	Solvents	— measurement
— bending	Toxic	
— compression	— asbestos	
— cutting, shearing	— heavy metals	
— gravitational pull	— inorganic toxicants	
— suspended mass	— organic toxicants	
— tension	— silica	
— torsion	**Immunological agents**	
Radiation energy	Allergenic	
Ionizing radiation	— antiseptic substances	
— accelerated particles (alpha particles, electrons, protons, neutrons)	— latex	
— gamma	Immunosuppressive	
— x-ray	Irritants	
Non-ionizing radiation	— cleaning residues	
— infrared	Sensitizing	
— laser		
— microwave		
— ultraviolet		
Thermal energy		
Cryogenic effects		
Hyperthermic effects		

© ISO 2019 – All rights reserved

C.3 Examples of events and circumstances

In order to identify foreseeable sequences of events, it is often useful to consider events and circumstances that can cause them. Table C.2 provides examples of events and circumstances, organized into general categories. Although the list is certainly not exhaustive, it is intended to demonstrate the many different types of events and circumstances that need to be taken into account to identify the foreseeable sequences of events for a *medical device*.

Table C.2 — Examples of events and circumstances

General category	Events and circumstances
Requirements	Inadequate specification of: — design parameters — operating parameters — performance requirements — in-service requirements (e.g. maintenance, reprocessing) — end of life
Manufacturing *processes*	Insufficient control of: — manufacturing *processes* — changes to manufacturing *processes* — materials — materials compatibility information — subcontractors
Transport and storage	Inadequate packaging Contamination or deterioration Inappropriate environmental conditions
Environmental factors	Physical factors (e.g. heat, pressure, time) Chemical factors (e.g. corrosion, degradation, contamination) Electromagnetic fields (e.g. susceptibility to electromagnetic disturbance) Inadequate supply of power Inadequate supply of coolant
Cleaning, disinfection and sterilization	Lack of validated *procedures* Inadequate specification of requirements Inadequate performance of cleaning, disinfection or sterilization
Disposal and scrapping	No or inadequate information provided *Use error*
Formulation	Biodegradation Biocompatibility No information or inadequate specification provided Incorrect formulations *Use error*

© ISO 2019 – All rights reserved

Table C.2 *(continued)*

General category	Events and circumstances
Usability	Confusing or missing instructions for use
	Complex or confusing control system
	Ambiguous or unclear state of the *medical device*
	Ambiguous or unclear presentation of settings, measurements or other information
	Misrepresentation of results
	Insufficient visibility, audibility or tactility
	Poor mapping of controls to actions, or of displayed information to actual state
	Controversial modes or mapping as compared to existing equipment
	Use by unskilled or untrained personnel
	Insufficient warning of side effects
	Inadequate warning of *hazards* associated with re-use of single-use *medical devices*
	Incorrect measurement and other metrological aspects
	Incompatibility with consumables, accessories, other *medical devices*
	Incorrect patient identification
	Slips, lapses and mistakes
Functionality	Loss of electrical or mechanical integrity
	Deterioration in performance (e.g. gradual occlusion of fluid or gas path, change in resistance to flow, electrical conductivity) as result of ageing, wear and repeated use
	Failure of a component due to ageing, wear or fatigue
Security	Unsecured data ports that are externally accessible (e.g. network, serial or USB ports)
	Data without encryption
	Software vulnerabilities that can be exploited
	Software updates without authenticity confirmation

C.4 Examples of relationships between *hazards*, foreseeable sequences of events, *hazardous situations* and the *harm* that can occur

Table C.3 illustrates the relationship between *hazards*, foreseeable sequences of events, *hazardous situations* and *harm* for some simplified examples. Remember that one *hazard* can result in more than one *harm* and that more than one sequence of events can give rise to a *hazardous situation*.

The decision on what constitutes a *hazardous situation* needs to be made to suit the particular analysis being carried out. In some circumstances it can be useful to describe a cover being left off a high voltage terminal as a *hazardous situation*, in other circumstances the *hazardous situation* can be more usefully described as when a person is in contact with the high voltage terminal.

© ISO 2019 – All rights reserved

Table C.3 — Relationship between *hazards*, foreseeable sequences of events, *hazardous situations* and the *harm* that can occur

Hazard	Foreseeable sequence of events	*Hazardous situation*	*Harm*
Electromagnetic energy (high voltage)	(1) Electrode cable unintentionally plugged into power line receptacle	Line voltage appears on electrodes	Serious burns Heart fibrillation
Chemical (volatile solvent, embolus)	(1) Incomplete removal of volatile solvent used in manufacturing (2) Solvent residue converts to gas at body temperature	Development of gas embolism (bubbles in the blood stream) during dialysis	Infarct Brain damage
Biological (microbial contamination)	(1) Inadequate instructions provided for decontaminating re-used anaesthesia tubing (2) Contaminated tubing used during anaesthesia	Bacteria released into airway of patient during anaesthesia	Bacterial infection
Functionality (no delivery)	(1) Electrostatically charged patient touches infusion pump (2) Electrostatic discharge (ESD) causes pump and pump alarms to fail	Failure to deliver insulin to patient with elevated blood glucose level, no warning given	Minor organ damage Decreased consciousness
Functionality (no output)	(1) Implantable defibrillator battery reaches the end of its useful life (2) Inappropriately long interval between clinical follow-up visits	Defibrillator cannot deliver shock when an arrhythmia occurs	Death
Measurement (incorrect information)	(1) Measurement error (2) No detection by user	Incorrect information reported to clinician, leading to misdiagnosis and/or lack of proper therapy	Progression of disease Serious injury

© ISO 2019 – All rights reserved

Bibliography

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

[2] ISO/IEC Guide 63:2019, *Guide to the development and inclusion of aspects of safety in international standards for medical devices*

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

[4] ISO 10993-1, *Biological evaluation of medical devices — Part 1: Evaluation and testing within a risk management process*

[5] ISO 13485:2016, *Medical devices — Quality management systems — Requirements for regulatory purposes*

[6] ISO 14155, *Clinical investigation of medical devices for human subjects — Good clinical practice*

[7] ISO 18113-1:2009, *In vitro diagnostic medical devices — Information supplied by the manufacturer (labelling) — Part 1: Terms, definitions and general requirements*

[8] ISO 20916, *In vitro diagnostic medical devices — Clinical performance studies using specimens from human subjects — Good study practice*

[9] ISO/TR 24971, *Medical devices — Guidance on the application of ISO 14971*

[10] ISO 31000, *Risk management — Guidelines*

[11] IEC/TR 60513, *Fundamental aspects of safety standards for medical electrical equipment*

[12] IEC 60601-1, *Medical electrical equipment — Part 1: General requirements for basic safety and essential performance*

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

© ISO 2019 – All rights reserved

ICS 11.040.01

Price based on 36 pages

© ISO 2019 – All rights reserved