[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.

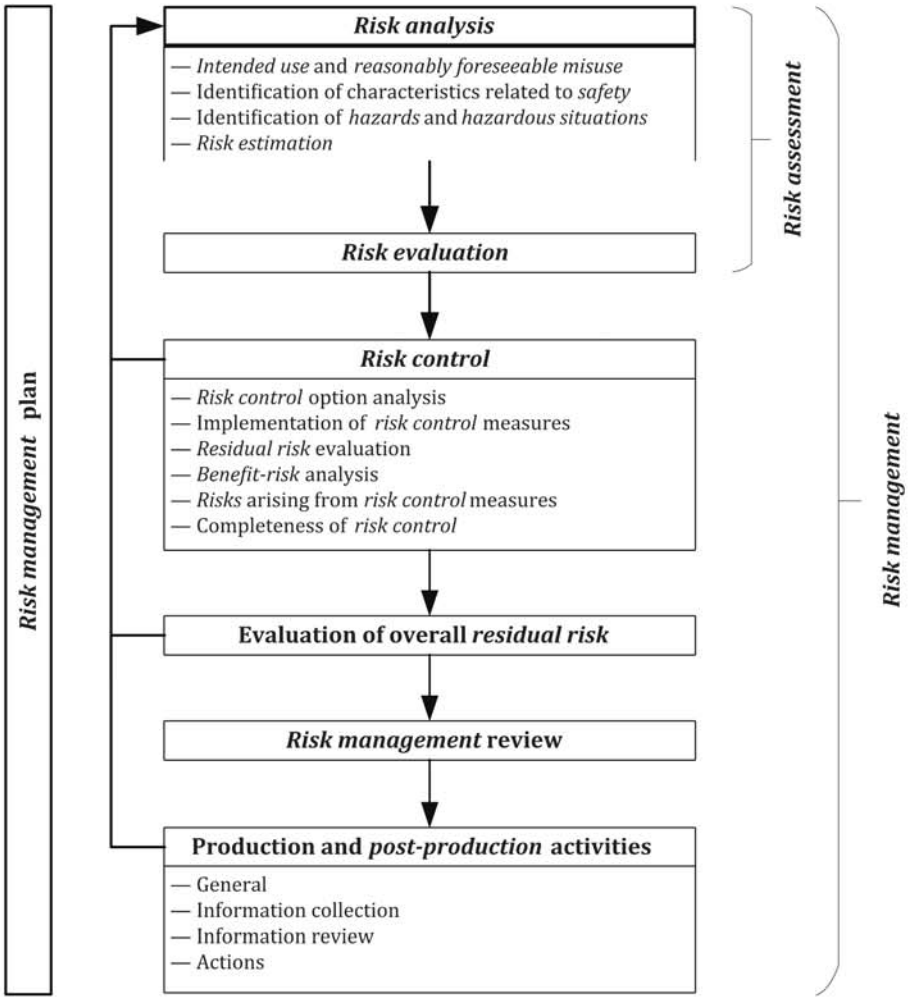

Figure 1 — A schematic representation of the *risk management process*

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*.

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*.

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.

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