D 54v19

Risk management of medical devices ISO 14971

Objective of the module: Risk control of medical devices (ISO 14971) to be able to:

- reduce risks
- obtain benefits greater than risks
- manage risks throughout the life cycle of the medical device

1 Risk

1.1 History

The word risk could come from the Latin word *resecum* “that which cuts, reef” hence the maritime origin “steep rock” or could derive from the ancient Italian *risicare*, which means “to dare.”

Opportunities and threats are two sides of the same coin called risk. When the outcome is favorable we speak of an opportunity, when the outcome is unfavorable we speak of a threat.

About 5,200 years ago in the Euphrates region, a group called Asipu were consultants in risk analysis for making risky or uncertain decisions.

Every decision involves risk. Peter Barge

In Mesopotamia, around 3,900 years ago insurance began as one of the oldest risk management strategies. The risk premium for ship and cargo losses in basic contracts was formalized in the Hamurabi Code.

More than 2,400 years ago Pericles spoke about taking risks and evaluating them before carrying out an action. His compatriot Socrates defines eikos (possible, probable) as “likelihood of truth”.

Blaise Pascal and Pierre de Fermat laid the foundations of probability theory in the 1650s, which opened the door to quantitative risk assessment.

Pierre Simon de Laplace developed a risk analysis in 1792 with his calculations of the probability of death with and without smallpox vaccination.

Risk management is relatively recent. For example, the Basel II agreement on risk management requirements in the banking sector dates from 2004. Some prescriptive (non-certifiable) standards on risk appeared at the beginning of the 21st century (see § 2.2).

In 1997, the European Committee for Standardization (ECS) published the standard EN 1441 “Medical devices – Risk analysis”.

In 1998, the ISO (International Organization for Standardization) published ISO 14971-1 – “Medical devices — Risk management — Part 1: Application of risk analysis” which became ISO 14971 in 2000. The second edition was released in 2007 and the third in 2019 (see § 2.2).

The ability to identify a hazard, analyze the risk, evaluate it, and then act accordingly is the basis of risk management.

A difficulty in risk management arises from the fact that the event concerned (the harm) takes place in the future. You have to imagine an event that may never take place.

Zero risk does not exist

For several decades, the majority of companies in the medical sector have become aware that the costs of implementing risk management are insignificant compared to the unfavorable consequences or even the insurance to take out.

The main objective of risk management is to ensure the survival of the company in all circumstances.

Risk management has been considered in the past by some managers as something superfluous, cf. annex 01. These people believed that the main goal was to avoid risk. Since then, many have understood that risk is inevitable and intrinsic to any activity but must be reduced to an acceptable level.

Risk cannot be eliminated

1.2 Scope

The scope of this module applies to risk management of medical devices (MDs). This concern:

- requirements (see chapter 4)
- risk analysis (see chapter 5)
- risk evaluation (see chapter 6)
- risk management (see chapter 7)
- the overall residual risk (see chapter 8)
- the risk management review (see chapter 9)
- production and post-production (see chapter 10)

The risk scope includes:

- the structure of the company
- the management system
- the department
- the process
- the product
- the service
- the project
- the performance
- reliability
- the costs
- the calendar
- the methods
- technology
- requirements
- specifications, including acceptance criteria
- functionalities
- the tools
- external providers
- the tests

This module does not specifically include risks related to:

- specific clinical procedures
- commercial activities
- accounting
- financial crises
- insurance
- natural disasters

- pandemics
- occupational diseases
- environmental protection
- food crises
- terrorist acts
- tax fraud
- counterfeit parts
- corruption

Risk management is used in many areas:

- insurance
- the bank
- the army
- energy
- aerospace
- projects
- medical devices
- medicine
- the company
- construction
- the markets

1.3 Benefits

Expected benefits of risk management of MDs:

- identification of hazards and their severity
- improved stakeholder confidence
- improvement of the overall performance of the company
- improvement of the company's reputation
- detection of potential future problems
- improved appreciation of opportunities and threats
- increased opportunities to achieve goals
- easier obtaining of the CE marking of a medical device (MD)
- creation of value for the company
- recalls avoided
- establishment of an adequate framework for the implementation in a controlled manner of any activity
- establishment of a reliable basis for decision-making
- identification of gaps
- obtaining a competitive advantage
- optimization of resource use
- protection of company assets
- effective response to changes
- reduction of costs and deadlines
- reduction of operational surprises
- scrupulous compliance with legal requirements
- increased visibility of the responsibilities of each staff member

The biggest risk is not taking any!

Root causes of failures:

- unplanned activities
- priority change
- irregular communication of results
- excessive self-confidence
- poorly defined acceptance criteria
- poorly understood requirements
- lack of resources
- poor estimation of effort
- poor distribution of work
- unplanned MD change
- new methods and technologies misunderstood
- unrealistic goals
- industrialization problems
- design issues
- unforeseen technical problems
- sporadic and inaccurate progress reports
- unidentified hazards
- insufficient support from top management
- conflicting or inconsistent specifications

Applying risk management upstream costs 10 times less than managing a crisis

The cost of managing risk over the life of a product is shown in figure 1-1.

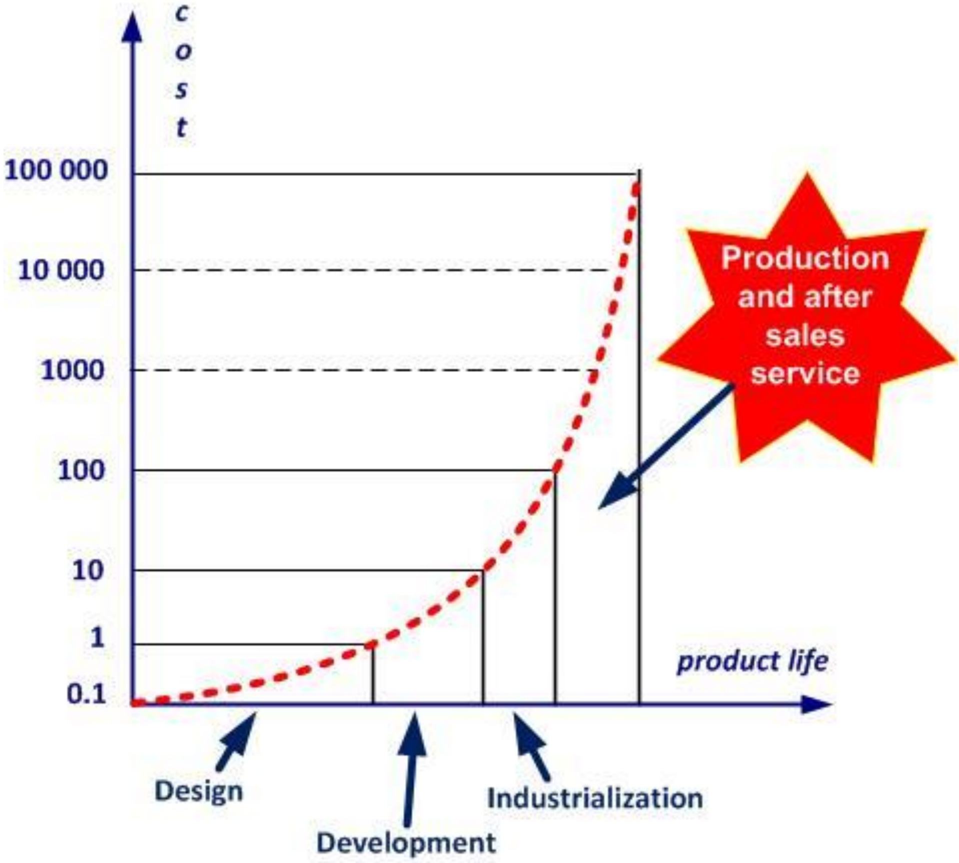


Figure 1-1. The cost and product cycle life

He who excuses himself, accuses himself

Common excuses for failure:

- it was the responsibility of top management
- this was not an explicit requirement in the contract
- how can we have an effective plan in the face of so many potential problems
- give me enough time and everything will be sorted
- in the event of a serious emergency situation, the implication will be completely different
- there was not enough time
- there was no staff available
- there are more important things to do
- I was sure we could cope
- I didn't realize it was so serious
- I didn’t think it was a key process
- I didn't think this would happen
- insurance had to take care of this situation
- the contract was already signed
- you cannot plan for the unexpected

2 Definitions, standards and books

2.1 Definitions

The beginning of wisdom is the definition of terms. Socrates

A risk can have negative impacts (we speak of threats) or positive impacts (we speak of opportunities).

Seizing an opportunity is taking risks, but not seizing an opportunity can expose us to risk.

Often risk is assimilated with hazard or danger and commonly used instead of threat.

There are multiple definitions of the word **risk**. Some examples:

- the likelihood that something will happen. IFRIMA (1994)
- combination of the probability of the occurrence of a dangerous event and the severity of the injury or harm to health caused to people by this event. ILO-OSH (2001)
- combination of the probability of an event and its consequences. ISO Guide 73 (2002)
- the possibility that something will happen that will impact the objectives. AS 4360 (2004)
- uncertainty of outcomes, whether a positive opportunity or a negative threat. OGC - UK (2005)
- effect of uncertainty on objectives. ISO Guide 73 (2009)
- description of a specific event that may or may not occur, as well as its causes and consequences. IRM (2013)
- effect of uncertainty. ISO 45001 (2018)
- combination of the probability of occurrence of harm and the severity of that harm. ISO 14971 (2019)
- the risk should be proportional to the probability of occurrence as well as the extent of damage. Blaise Pascal
- possible hazard, more or less predictable. Little Robert
- negative effect of uncertainty. Christopher Paris
- mathematical expectation of an event probability function. Daniel Bernoulli
- event whose random occurrence is likely to cause damage to people or property or both at the same time. Serge Braudo
- the extent of the potential loss. Evan Picoult
- the future impact of an uncontrolled danger. Sean Chamberlin
- the extent of the danger. Georges-Yves Kervern
- probability and magnitude of a loss, disaster or other adverse event. Douglas Hubbard

Our preference:

Risk: *likelihood of occurrence of a threat or an opportunity*

Some definitions of **risk management**:

- coordinated activities to direct and control an organization with regard to risk. ISO Guide 73 (2009)
- systematic application of management policies, procedures and practices to analysis, evaluation, control and risk management tasks. ISO/IEC 63 (2019)

- culture, processes and structures in place to effectively manage opportunities and negative impacts. Business Continuity Institute
- be smart to take risks. Douglas Hubbard
- provides a framework for organizations to control and respond to uncertainties. Paul Hopkins
- the act or practice of risk. Edmund Conrow

Our preference:

Risk management: *activities to restrict the possibility that something goes wrong*

Some definitions of the word **hazard** (or hazardous situation):

- source or situation likely to cause trauma and pathologies. ISO 45001 (2018)
- source of potential harm. ISO/IEC Guide 63 (2019)
- what constitutes a threat, a risk for someone, something. Larousse
- what threatens or compromises the safety or existence of a person or thing. Little Robert
- intrinsic property of a substance, of a system which can lead to damage. Yvan Vérot

Our preference:

Hazard: *situation that could lead to an incident*
Identify the hazard: *ask yourself what could go wrong*

Some definitions of **risk evaluation**:

- overall process of risk identification, risk analysis and risk evaluation. ISO Guide 73 (2009)
- overall process comprising a risk analysis and a risk evaluation. ISO/IEC Guide 51 (2014)
- assessment of undesirable outcomes and assigning probabilities to their chances of occurrence. Vlasta Molak
- qualitative and quantitative risk assessment process and determination of the type of analysis to be carried out. Quebec Office of the French Language

Our preference:

Risk evaluation: *process of risk identification, analysis and evaluation*

Some definitions of risk identification:

- process of finding, recognizing and describing risks. ISO Guide 73 (2009)
- process for reviewing program areas and each critical technical process to identify and document associated risk. Edmund Conrow

Our preference:

Risk identification: *assessment activity to find and describe risks*

Some definitions of **risk analysis**:

- process to comprehend the nature of risk and to determine the level of risk. ISO Guide 73 (2009)

- systematic use of available information to identify hazards and to estimate the risk. ISO Guide 63 (2019)
- process of examining each identified risk issue or process to refine the description of the risk, isolate the cause and determine the effects. Edmund Conrow
- systematic use of information to identify sources and assign risk values. Terje Aven

Our preference:

Risk analysis: *activity to understand the nature of a risk and determine its impact*

Some definitions of **risk treatment**:

- process of developing, selecting and implementing controls. BS 31100 (2011)
- process to modify risk. ISO Guide 73 (2009)
- process that identifies, evaluates, selects and implements options to set risk at acceptable levels given the constraints and objectives of the program. Edmund Conrow

Our preference:

Risk treatment: *risk modification activities*

Some definitions of the word **opportunity**:

- positive effect of uncertainty. Christopher Paris
- potential for achieving desired and positive outcomes of an event. Robert Charrette

Our preference:

Opportunity: *uncertain event that may have a favorable impact*

Uncertainty and probability (likelihood) are subjective notions with invented quantities.

Impact: *consequence of an event affecting the objectives*

Likelihood: *possibility that something happens*

Probability can be considered as a measure of uncertainty. If probability can be measured it is therefore linked to something that has happened. Likelihood is a more general notion because it can include an effect that never happened.

To avoid confusing hazard and risk, a few simple examples:

Hazard	Risk
slippery floor	broken leg
electricity	electrocution
tobacco	lung cancer
climb a ladder	break your arm when falling

Risk depends on its context. Example:

- driving a car in town involves a minimal risk of accident
- driving a car in the city, but in a country in civil war, can lead to irreparable harm

As shown in figure 2-1, the time of exposure to hazard multiplies the risk:

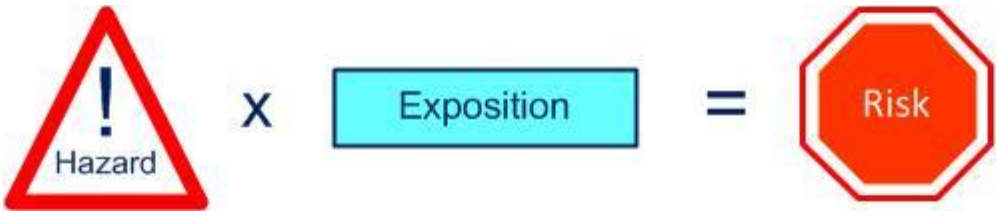


Figure 2-1. Exposure to hazard

Risk (and its level) is a function of impact and likelihood of occurrence (figure 2-2).

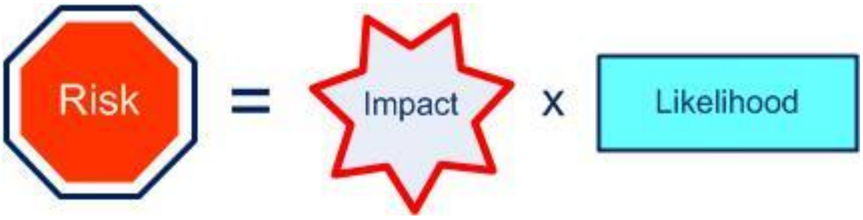


Figure 2-2. The level of risk

The risk is residual when the impact and likelihood of occurrence are low, cf. figure 2-3. As soon as the impact and likelihood are high, we approach the critical zone (red).

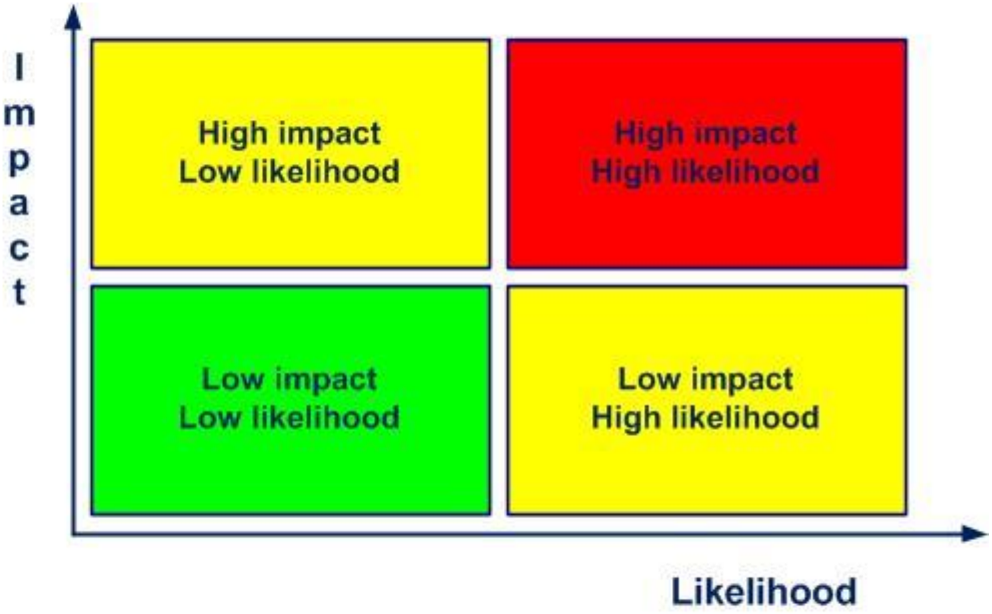

Impact
High impact Low likelihood
High impact High likelihood
Low impact Low likelihood
Low impact High likelihood
Likelihood

Figure 2-3. The criticality of the risk

More details on risk levels are shown in annex 02.

Some definitions and acronyms:

Attitude towards risk: *evaluating and treating risk*

Benchmarking: *comparative analysis technique against one or more competitors*

Brainstorming: *method allowing the development of ideas from the participants in order to find solutions*

Business continuity management*: method aimed at ensuring that in the event of a crisis, critical functions remain operational or become operational again as quickly as possible (see also resilience)*

Business continuity plan: *business continuity management planning including approach, steps, methods, resources*

Conformity: *fulfillment of a specified requirement*

Control plan*: document describing the specific measures to carry out the control of a product or process*

Control: *see inspection*

Corrective action: *action to eliminate the causes of nonconformity or any other undesirable event and to prevent their recurrence*

Criticality*: level of a potential risk*

Customer: *anyone who receives a product*

Effectiveness: *capacity to perform planned activities with minimum effort*

Efficiency: *financial relationship between achieved results and resources used*

Harm: *bodily injury or damage to human health, property or the environment*

Inspection: *actions of measuring, testing and reviewing a product, service, process or material to determine compliance with requirements*

ISO: *international organization for standardization*

Kaizen: *from Japanese, kai = change and zen = good (for the better, better), Kaizen = continual improvement*

Level of risk: *criticality of the risk based on impact and likelihood*

Life cycle: *all phases in the life of a product from design to disposal*

Management system: *set of processes allowing objectives to be achieved*

Manager: *someone who gets results through other people*

Manufacturer: *person or group responsible for the design, manufacturing, packaging and labeling of a good*

MCT: *multiple choice test*

Medical device (MD): *product or service used for the purposes of diagnosis, prevention, monitoring, treatment, mitigation of disease or injury*

Monitoring: *set of planned actions to guarantee the effectiveness of control measures*

MS: *management system*

Nonconformity (NC): *non-fulfillment of a specified requirement*

Non-quality: *gap between expected and perceived quality*

Organization: *structure that satisfies a need*

Preventive action: *action to eliminate the potential causes of nonconformity or any other undesirable event and to prevent their appearance*

Problem: *gap that must be reduced to obtain a result*

Process: *activities that transform input into output*

Product (or service): *any result of a process or activity*

QM: *quality manager*

Requirement: *implicit or explicit need or expectation*

Residual risk*: acceptable risk following the implementation of risk control measures*

Resilience: *ability to resolve a crisis and continue operating as before*

Responsibility: *capacity to make a decision alone*

Risk control*: risk reduction activities*

Risk criteria*: indices to evaluate the importance of risk*

Risk factor (peril, danger): *element likely to cause a risk*

Risk management plan: *risk management planning including approach, steps, methods, resources*

Risk management system: *set of processes enabling risk objectives to be achieved*

Risk measure: *set of possibilities with quantified probabilities and losses*
Risk owner*: person with responsibility and authority to control risk*
Risk prevention: *activities to reduce the likelihood of risk occurrence*
Risk protection*: activities to reduce risk impacts*
Risk register*: folder containing information relating to identified risks*
Risk severity: *measuring the impact of risk*
Risk threshold*: acceptance limit (below) or non-tolerance limit (above)*
RMS*: risk management system*
Safety: *lack of unacceptable risk*
Stakeholder*: person, group or company that can affect or be affected by an organization*
Strategy: *total approach to achieve objectives*
Supplier: *entity that provides a product*
System: *set of interacting processes*
Threat: *uncertain event that could have a negative impact on the objectives*
Top management (direction): *group or persons responsible for management at the highest level of the company*
Uncertainty*: existence of more than one possibility*
Waste: *anything that adds cost but not value*

In the terminology of management systems, do not confuse:

- accident and incident
  - an accident is an unexpected serious event
  - an incident is an event that can lead to an accident
- anomaly, defect, dysfunction, failure, nonconformity, reject and waste:
  - an anomaly is a deviation from what is expected
  - a defect is the non-fulfillment of a requirement related to an intended use
  - a dysfunction is a degraded function that can lead to a failure
  - a failure is when a function has become unfit
  - a nonconformity is the non-fulfillment of a requirement in production
  - a reject is a nonconforming product that will be destroyed
  - a waste is when there are added costs but no value
- audit program and plan
  - an audit program is the annual planning of the audits
  - an audit plan is the description of the audit activities
- audit, inspection, auditee and auditor
  - an audit is the process of obtaining audit evidence
  - an inspection is the conformity verification of a process or product
  - an auditee is the one who is audited
  - an auditor is the one who conducts the audit
- control and optimize
  - to control is to meet the objectives
  - to optimize is to search for the best possible results
- customer, external provider and subcontractor
  - a customer receives a product
  - an external provider provides a product on which specific work is done
  - a subcontractor provides a service or product on which specific work is done
- effectiveness and efficiency
  - effectiveness is the level of achievement of planned results
  - efficiency is the ratio between results and resources

- follow-up and review
    - follow-up is the verification of the obtained results of an action
    - review is the analysis of the effectiveness in achieving objectives
- hazard, problem and risk
    - hazard is the state, the situation or the source that can lead to an accident
    - problem is the gap between the actual situation and the desired situation
    - risk is the measure, the consequence of a hazard and it is always a potential problem
- inform and communicate
    - to inform is to give someone meaningful data
    - to communicate is to pass on a message, to listen to the reaction and discuss
- objective and indicator
    - an objective is a sought-after commitment
    - an indicator is the information on the difference between the pre-set objective and the achieved result
- organization and enterprise, society, company
    - organization is the term used by the ISO 9001 standard as the entity between the supplier and the customer
    - an enterprise, society and company are examples of organizations
- prevention and protection, cf. figure 2-4
    - prevention is the means to reduce the likelihood and frequency of occurrence of a risk (checking tire pressure)
    - protection is the means to limit the impact of a risk (fastening your seat belt)
- process, procedure, product, activity and task
    - a process is how we satisfy the customer using people to achieve the objectives
    - a procedure is the description of how we should conform to the rules
    - a product is the result of a process
    - an activity is a set of tasks
    - a task is a sequence of simple operations
- risk and crisis management
    - risk management is like fire prevention
    - crisis management is like putting out a fire

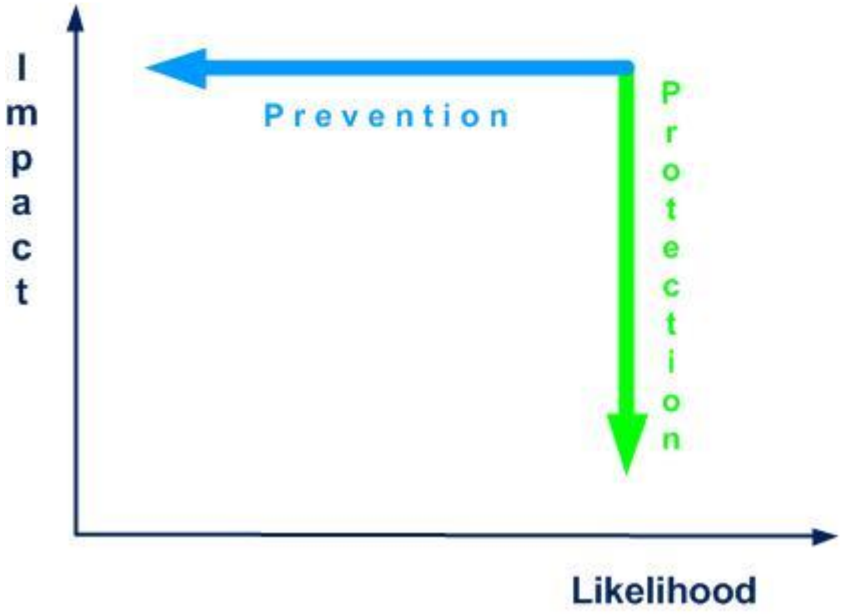


Figure 2-4. Prevention and protection

Remark 1: the most important thing is to determine a common and unequivocal vocabulary for everyone in the company.

Remark 2: between likelihood and probability our preference is for likelihood.

Remark 3: the customer can also be the user, the beneficiary, the trigger, the ordering party or the consumer.

Remark 4: each time you use the expression "opportunity for improvement" instead of nonconformity, malfunction or failure, you will gain a little more trust from your interlocutor (external or internal customer).

For other definitions, comments, explanations and interpretations that you don't find in this module and in annex 06, you can consult:

- ISO Online Browsing Platform (OBP)
- IEC Electropedia

2.2 Standards

Risk-related standards (in chronological order):

- AS 4360 (1995): Risk management
- IRM/Alarm/AIRMIC (2002): A Risk Management Standard (Risk Management Reference Framework)
- FD X50-117 (2003): Project management - Risk management - Project risk management
- IEC 60601-1 (2005): Medical electrical equipment - Part 1: General requirements for basic safety and essential performance
- FD X50-252 (2006): Risk management - Guidelines for risk estimation
- IEC 62304 (2006): Medical device software - Software life cycle processes
- BS 31100 (2008): Risk management - code of practice
- 768/2008/CE: Uniform conditions for the marketing of safe products in the EU (conformity marking)
- ISO Guide 73 (2009): Risk management - Vocabulary
- FD X50-253 (2011): Risk management - Risk management process - Guidelines for communication
- BP Z74-700 (2011): Business Continuity Plan (BCP)
- NF S99-170 (2013): Maintenance of medical devices - Quality management system for the maintenance of medical devices and the management of risks associated with their use
- FD ISO 31004 (2014): Risk management - Guidelines for the implementation of ISO 31000
- FD X50-259 (2014): Risk management - Business continuity plan (PCA) - Implementation and maintenance approach
- IEC 62366-1 (2015): Medical devices - Part 1: Application of usability engineering to medical devices
- ISO 13485 (2016): Medical devices - Quality management systems - Requirements for regulatory purposes
- FD X50-260 (2016): Risk management - Guidelines for implementation in ETI/SMEs and other organizations - ETI/SME-PMI

- 2017/745 (2017): Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices
- NF S99-172 (2017): Use and maintenance of medical devices - Risk management system for risks associated with the use of medical devices
- ISO 31000 (2018): Risk management – Guidelines
- ISO 10993-1 (2018): Biological evaluation of medical devices - Part 1: Evaluation and testing within a risk management process
- NF EN ISO 14971 (2019): Medical devices - Application of risk management to medical devices
- IEC 31010 (2019): Risk management - Risk assessment techniques
- ISO Guide 63 (2019): Guide to the development and inclusion of aspects of safety in International Standards for medical devices
- ISO 20916 (2019): In vitro diagnostic medical devices - Clinical performance studies using specimens from human subjects - Good study practice
- ISO/TR 24971 (2020): Medical devices - Guidance on the application of ISO 14971
- ISO/TR 20416 (2020): Medical devices - Post-market surveillance for manufacturers
- XP S99-223 (2020): Medical Device - Benefit risk management
- ISO 14155 (2020): Clinical investigation of medical devices for human subjects - Good clinical practice
- BS 31100 (2021): Risk management. Code of practice
- ISO 20417 (2021): Medical devices - Information to be supplied by the manufacturer
- ISO 10017 (2021): Quality management - Guidance on statistical techniques for ISO 9001:2015

Two French documents related to the processes with explanations, recommendations and examples:

- AC X50-178 (agreement, 2002) Quality management – Process management – Good practices and feedback
- FD X50-176 (documentation booklet, 2017) Management tools – Process management

Risk management – ENA – 2020 bibliography.

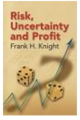
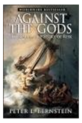
None of these standards are obligatory but as Deming said:

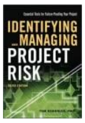
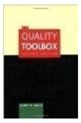
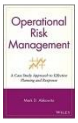
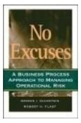
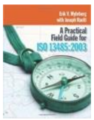
There is no need to change. Survival is not obligatory

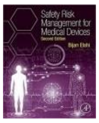
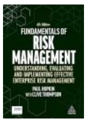
2.3 Books

When I think of all the books still left for me to read, I am certain of further happiness. Jules Renard

To go further, some books, classified in chronological order:

-  Frank Knight, Risk, Uncertainty And Profit, University of Chicago Press, 1921
-  Peter Bernstein, Against the Gods: The Remarkable Story of Risk, John Wiley & Sons, New York, 1998

- Michael Gallagher, Business Continuity Management - How to Protect Your Company from Danger, Prentice Hall, 2002
- Edmund Conrow, Effective Risk Management: Some Keys to Success, AIAA, 2003
-  Tom Kendrick, Identifying and managing project risk: Essential Tools for Failure-Proofing Your Project, AMACOM, 2003
-  Nancy Tague, The Quality Toolbox, ASQC Quality Press, 2005
-  Mark Abkowitz, Operational risk management, Wiley, 2008
-  Dennis Dickstein, No excuses, A business process approach to managing operational risk, Wiley, 2009
- team, Management of Risk: Guidance for Practitioners, Stationery Office Books, 2010
- Torben Andersen, Strategic Risk Management Practice: How to Deal Effectively with Major Corporate Exposures, Cambridge University Press, 2010
- Antonio Borghesi, Barbara Gaudenzi, Risk Management, How to Assess, Transfer and Communicate Critical Risks, Springer, 2013
-  Eric Myhrberg, A Practical Field Guide for Iso 13485 2003, ASQ, 2013
- Karl Weick, Kathleen Sutcliffe, Managing the Unexpected: Sustained Performance in a Complex World, Wiley, 2015
- ISO 31000 - Risk Management - A practical guide for SMEs, ISO, 2015
- Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, Deputy Assistant Secretary of Defense Systems Engineering, 2017

- COSO, Enterprise Risk Management - Integrating with Strategy and Performance, AICPA, 2017
- Greg Hutchins, ISO 31000: 2018 Enterprise Risk Management, Certified Enterprise Risk Manager (R) Academy, 2018
- AICPA, Practice Aid: Enterprise Risk Management: Guidance For Practical Implementation and Assessment, 2018, Wiley, 2018
- Dyadem, Guidelines for Failure Mode and Effects Analysis for Medical Devices, CRC Press, 2018
- James Kline, Enterprise Risk Management in Government: Implementing ISO 31000:2018, Quality Plus Engineering, 2019
- ISO 31000 Risk Management A Complete Guide - 2021 Edition, The Art of Service, 2020
- Amir Samimi, A Review of Risk Management According to ISO 31000, 2018, Scholars' Press, 2020
- Douglas W. Hubbard, The Failure of Risk Management: Why It's Broken and How to Fix It 2nd Edition, Wiley, 2020
- Gerardus Blokdyk, ISO 14971 A Complete Guide - 2021 Edition, 5STARCooks, 2020
- Gerardus Blokdyk, ISO 13485 A Complete Guide - 2020 Edition, 5STARCooks, 2020
-  Bijan Elahi, Safety Risk Management for Medical Devices, Academic Press, 2021
-  Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Enterprise Risk Management 6th Edition, Kogan Page, 2021

- Jennifer Geary, How to be a Chief Risk Officer: A handbook for the modern CRO, Neilsen, 2022

None of these books are mandatory...

3 Process approach

If you cannot describe what you are doing as a process, you do not know what you're doing. Edwards Deming

3.1 Process types

The word process comes from the Latin root procedere = go, development, progress (Pro = forward, cedere = go). Each process transforms inputs into outputs, creating added value and potential nuisances.

A process has three basic elements: inputs, activities and outputs.

A process can be very complex (launch a rocket) or relatively simple (audit a product). A process is:

- repeatable
- foreseeable
- measurable
- definable
- dependent on its context
- responsible for its external providers

A process is, among other things, determined by its:

- title and its type
- purpose (why?)
- beneficiary (for whom?)
- scope and activities
- initiators
- documents and records
- inputs
- outputs (intentional and unintentional)
- restrains
- people
- material resources
- objectives and indicators
- person in charge (owner) and actors (participants)
- means of inspection (monitoring, measurement)
- mapping
- interaction with other processes
- risks and potential deviations
- opportunities for continual improvement

A process review is carried out periodically by the process owner (cf. annex 03).

The components of a process are shown in figure 3-1:

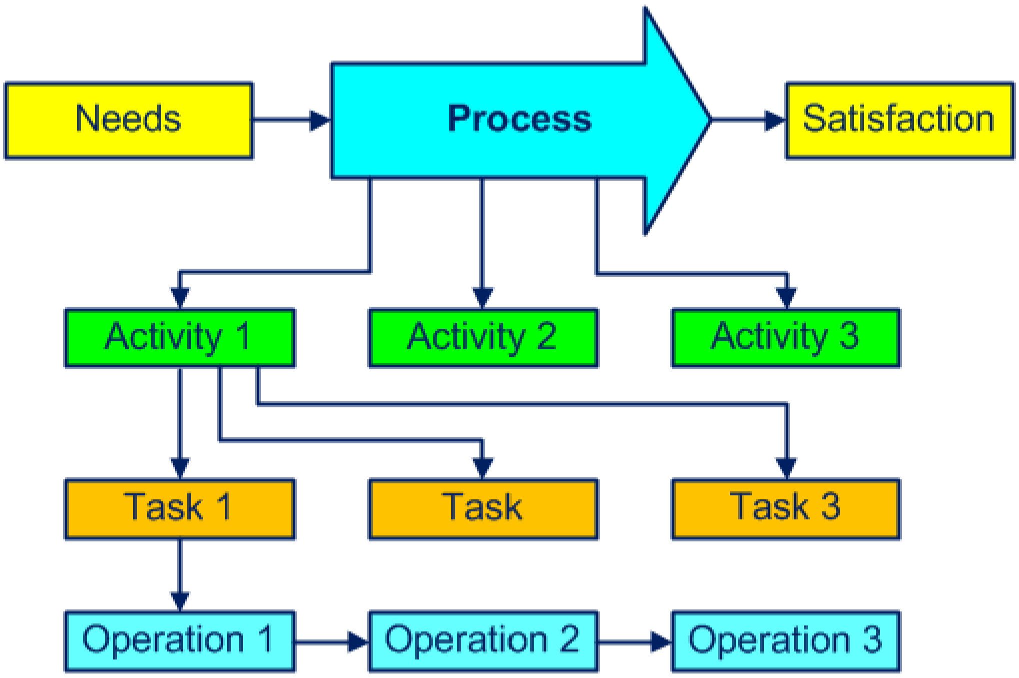


Figure 3-1. Components of a process

Figure 3-2 shows an example that helps answer the questions:

- which materials, which documents, which tooling? (inputs)
- which title, which activities, requirements and constraints? (process)
- which products, which documents? (outputs)
- how, which inspections? (methods)
- what is the level of performance? (indicators)
- who, with what competence? (staff)
- with what, which machines, which equipment? (material resources)

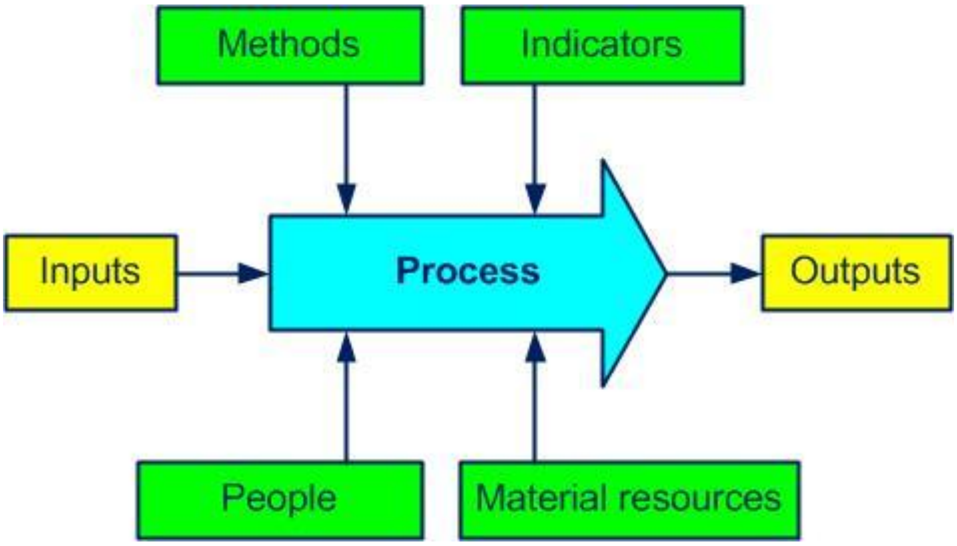


Figure 3-2. Some elements of a process

Often the output of a process is the input of the next process.

You can find some examples of process forms in the document pack D 02.

Any organization (company) can be considered as a macro process, with its purpose, its inputs (customer needs and expectations) and its outputs (products/services to satisfy customer requirements).

Our preference is to identify a process using a verb (buy, produce, sell) instead of a noun (purchases, production, sales) to differentiate the process from the company's department or procedure to maintain and recall the purpose of the process.

The processes are (as we will see in the following paragraphs) of management, realization and support types. Do not attach too much importance to process categorizing (sometimes it is very relative), but ensure that all the company's activities at least fall into one process.

3.1.1 Management processes

Management processes are also known as piloting, decision, key or major processes. They take part in the overall organization and include the development of the policy, deployment of the objectives and all needed checks. They are the glue of all realization and support processes.

The following processes can be part of this family:

- develop strategy
- address MD risks, cf. annex 04:
  - plan
  - assess:
    - identify
    - analyze
    - evaluate
  - treat
- develop policy
- establish process ownership
- improve
- audit
- communicate
- plan the MS
- acquire resources
- negotiate contract
- analyze data

3.1.2 Realization processes

The realization (operational) processes are related to the product, increase the added value and contribute directly to customer satisfaction.

They are mainly:

- design and develop new products
- purchase components
- produce products
- sell products
- inspect production
- maintain equipment
- implement traceability (identify and keep history)

- receive, store and deliver
- control nonconformities
- implement preventive and corrective actions
- monitor post-market, cf. annex 05
- evaluate benefit-risk ration, cf. annex 07

3.1.3 Support processes

The support processes provide the resources necessary for the proper functioning of all other processes. They are not directly related to a contribution of the product's added value but are still essential.

The support processes are often:

- control documentation
- provide information
- acquire and maintain infrastructure
- provide training
- manage inspection means
- manage staff
- keep accountability

3.2 Process mapping

Par excellence process “mapping” is a multidisciplinary work. This is not a formal requirement of the ISO 14971 standard but is always welcome.

The three types of processes and some interactions are shown in figure 3-3 and D 02.

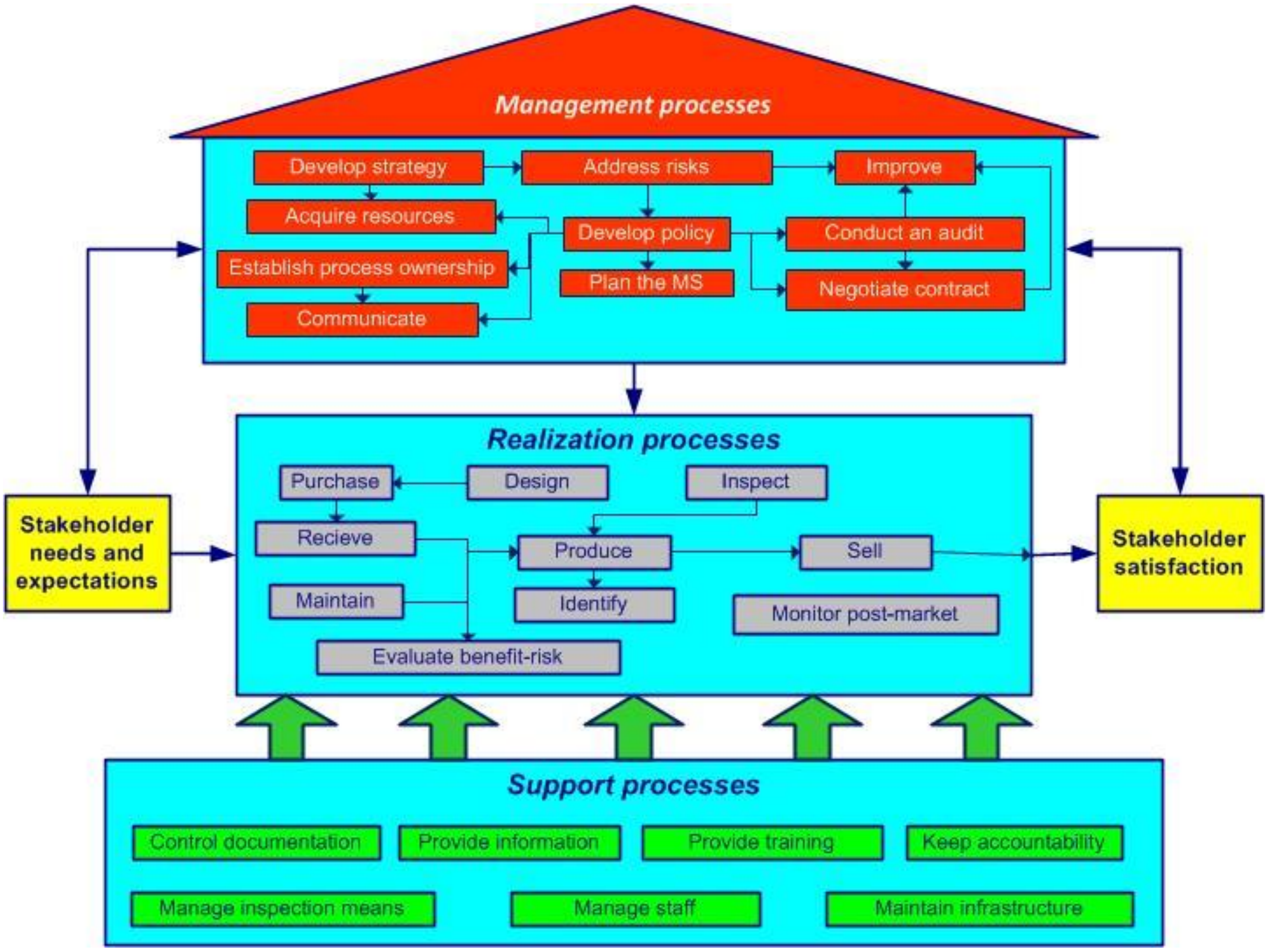


Figure 3-3. Process house

Mapping, among other things, allows you to:

- obtain a global vision of the company
- identify the beneficiaries (customers), flows and interactions
- define (simple) rules for communication between processes

To obtain a clearer picture, you can simplify by using a total of about 15 core processes. A core process can contain several sub-processes: for example, the process "develop the MS" can involve:

- develop strategy
- manage risks
- develop policy
- plan the MS
- deploy objectives
- acquire resources
- establish process ownership
- improve

3.3 Process approach

Simple solutions for now, perfection for later

The fourth principle of quality management is “Process approach” (see ISO 9000, 2.3.4). Some benefits:

- obtain a global vision of the company thanks to the mapping
- identify and manage responsibilities and resources
- achieve effective management of the company based on process indicators
- manage risks that could influence the objectives

Process approach: *management by the processes to better satisfy customers, improve the effectiveness of all processes and increase global efficiency*

When the process approach is integrated during the development, implementation and continual improvement of a management system, it allows one to achieve objectives that are related to customer satisfaction, as is shown in figure 3-4 (cf. ISO 9001, 0.2).

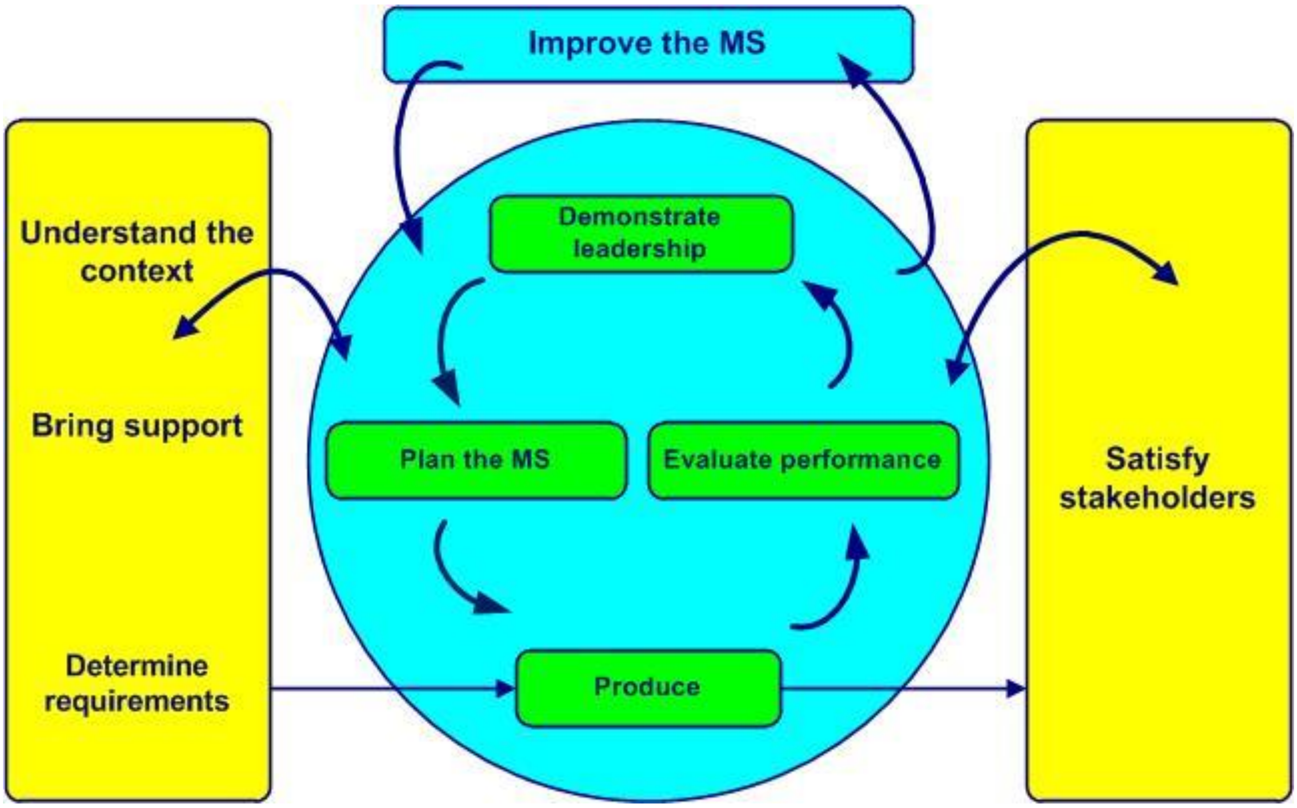


Figure 3-4. Model of an MS-based on the process approach and continual improvement

The process approach (cf. annex 08):

- emphasizes the importance of:
    - understanding and complying with customer requirements
    - prevention so as to react to unwanted elements such as:
        - customer returns
        - waste
    - measuring process performance, effectiveness and efficiency
    - permanently improving objectives based on pertinent measurements
    - process added value
- relies on:
    - methodical identification
    - interactions

    - the sequence and
  - process management, which consists of:
    - determining objectives and their indicators
    - piloting related activities
    - analyzing obtained results
    - permanently undertaking improvements
- allows one to:
  - better view inputs and outputs and their relationship
  - clarify roles and responsibilities
  - judiciously assign necessary resources
  - break down barriers between departments
  - decrease costs, delays and waste
- and ensures in the long run:
  - control
  - monitoring and
  - continual improvement of processes

The process approach **is not**:

- crisis management ("You will not solve the problems by addressing the effects")
- blaming people (“Poor quality is the result of poor management" - Masaaki Imai)
- prioritizing investments (“Use your brain, not your money" - Taiichi Ohno)

The PDCA cycle, also called the Deming cycle, applies to the control of any process, including the integration of risk management into the framework of the company. The PDCA cycles (Plan, Do, Check, Act) are a universal basis for continual improvement (see figure 3-5).

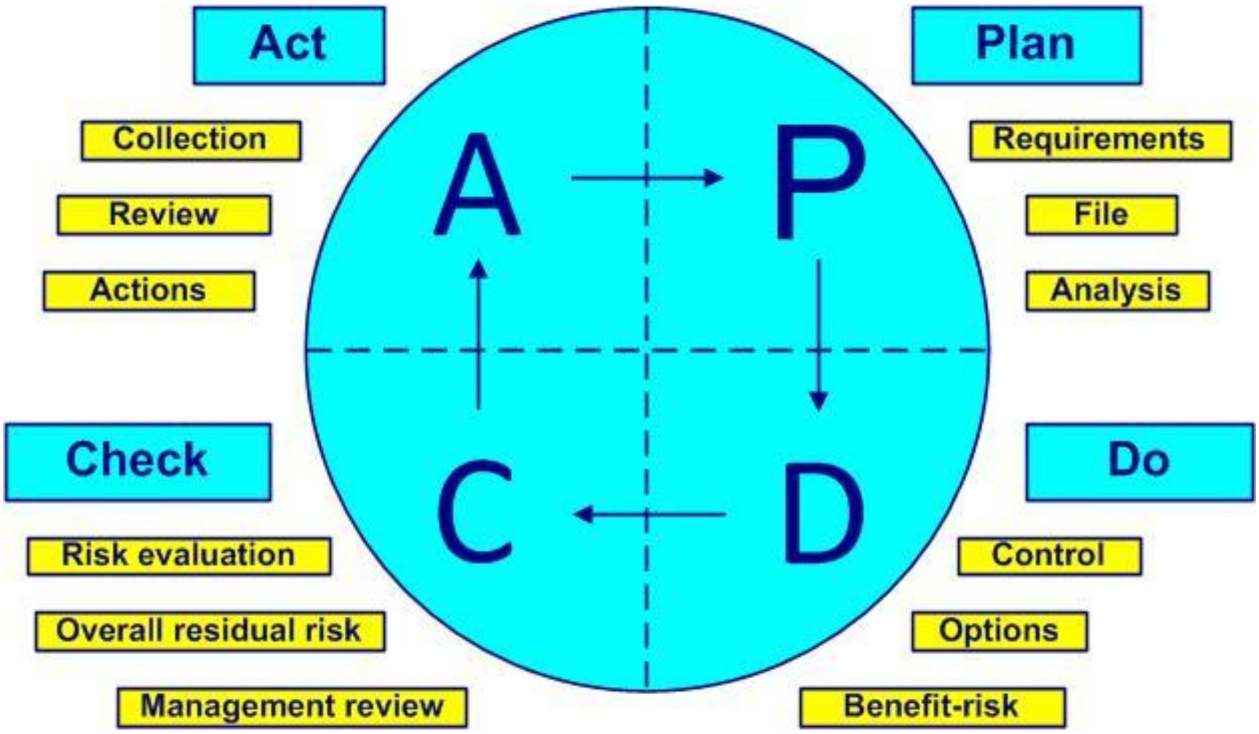


Figure 3-5. The Deming cycle for risk management

- Plan – define requirements, demonstrate leadership, establish the risk management file, analyze risks, identify hazards (clauses 4, and 5)

- Do – control risks, choose options for risk control measures, analyze benefits in relation to risks (clause 7)
- Check – verify, evaluate risk, evaluate overall residual risk, review risk management (clauses 6, 8 and 9)
- Act – collect feedback, review the information collected, take necessary actions (clause 10)

To learn more about the Deming cycle and its 14 points of management theory, you can consult the book “Out of the Crisis” W. Edwards Deming, Economica, 2002, first published in 1982.

Minute of relaxation. Paganini's violin concert performed with facial expressions.

4 General requirements

4.1 Risk management

Requirements 1 to 11

The requirements of ISO 14971 in clauses 4 to 10 are shown in figure 4-1:

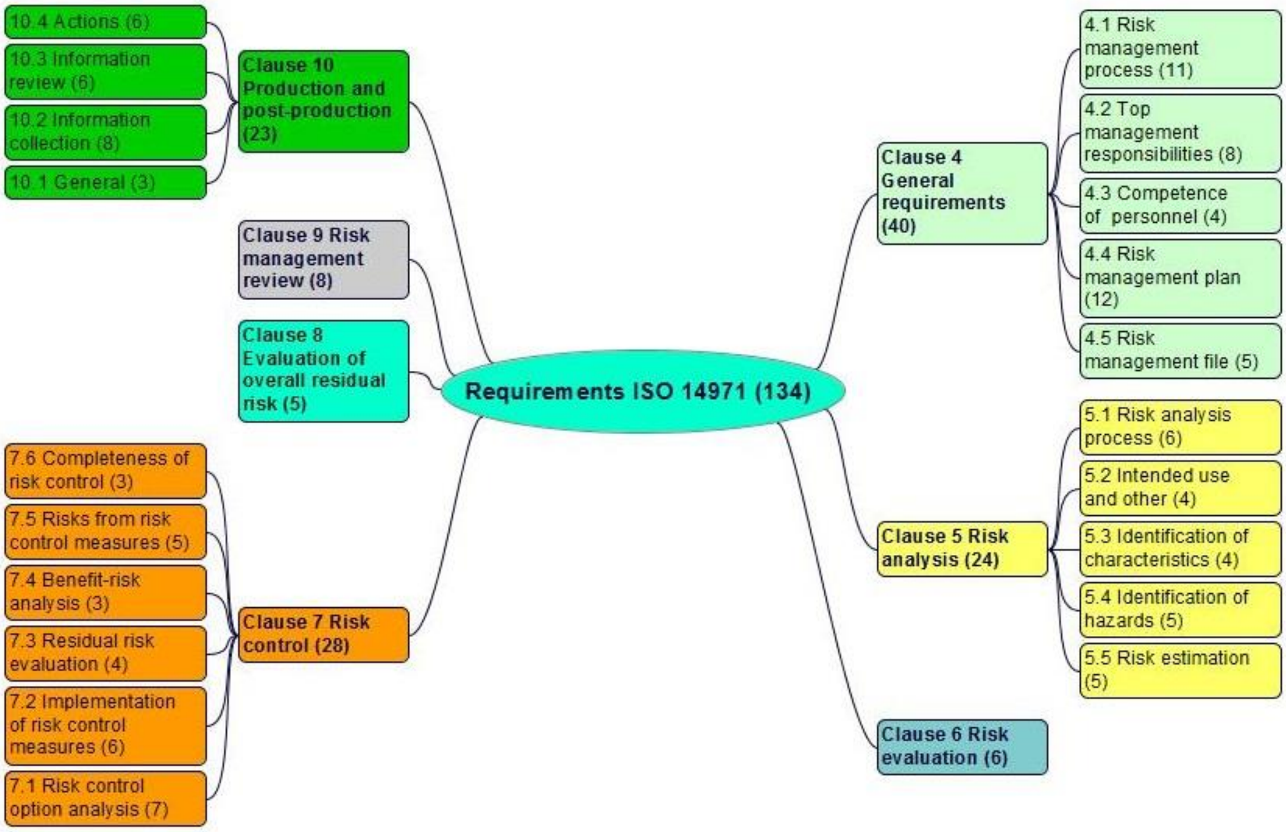

10.4 Actions (6)
10.3 Information review (6)
10.2 Information collection (8)
10.1 General (3)
Clause 10 Production and post-production (23)
Clause 9 Risk management review (8)
Clause 8 Evaluation of overall residual risk (5)
Requirements ISO 14971 (134)
7.6 Completeness of risk control (3)
7.5 Risks from risk control measures (5)
7.4 Benefit-risk analysis (3)
7.3 Residual risk evaluation (4)
7.2 Implementation of risk control measures (6)
7.1 Risk control option analysis (7)
Clause 7 Risk control (28)
Clause 4 General requirements (40)
4.1 Risk management process (11)
4.2 Top management responsibilities (8)
4.3 Competence of personnel (4)
4.4 Risk management plan (12)
4.5 Risk management file (5)
Clause 5 Risk analysis (24)
5.1 Risk analysis process (6)
5.2 Intended use and other (4)
5.3 Identification of characteristics (4)
5.4 Identification of hazards (5)
5.5 Risk estimation (5)
Clause 6 Risk evaluation (6)

Figure 4-1. Requirements of ISO 14971

These requirements allow MD manufacturers to:

- identify hazards
- estimate and evaluate risks
- control risks and
- monitor the effectiveness of the risk control measures put in place

Risk is everyone’s business

Integrating risk management into all company processes is a key objective.

The requirements apply to all stages of the life cycle of MDs and to the risks associated with a MD such as:

- biocompatibility
- information security
- electricity
- moving parts
- radiation
- normal use

- reasonably foreseeable misuse, cf. § 5.2

When a requirement is linked to a risk control measure, it becomes a safety requirement for the medical device.

The “Manage risks of a medical device” process and the clauses of ISO 14971 are shown in figure 4-2, cf. annex 04:

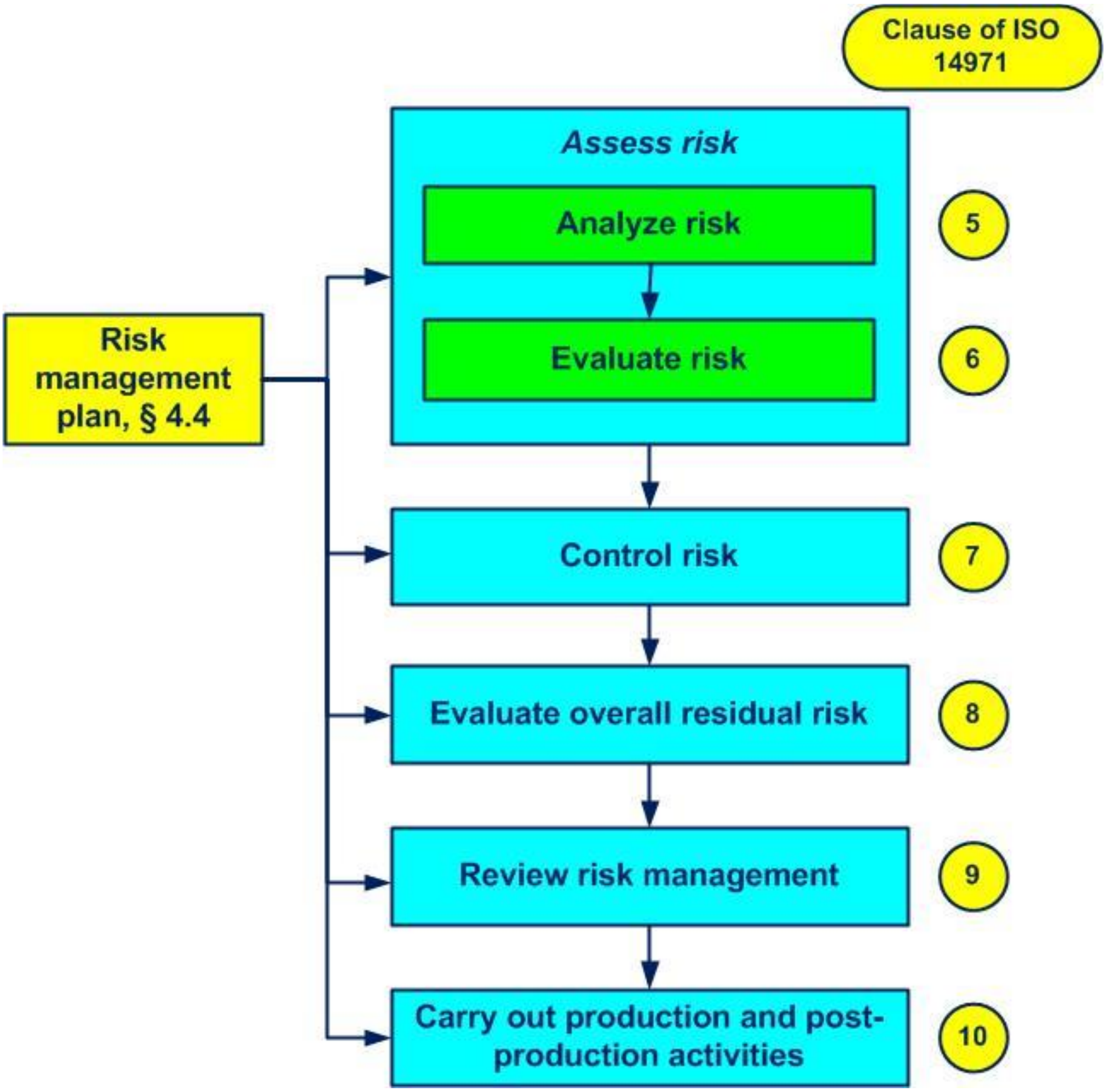

Clause of ISO 14971
Risk management plan, § 4.4
Assess risk
Analyze risk
5
Evaluate risk
6
Control risk
7
Evaluate overall residual risk
8
Review risk management
9
Carry out production and post-production activities
10

Figure 4-2. Manage risks of an MD

The “Risk management” procedure allows you to follow the essential steps, cf. annex 09.

The “Risk Support”, in Excel format, allows you to identify, analyze, evaluate and treat DM risks, cf. annex 10.

The “Address MD risks” process can also be represented as follows (figure 4.3):

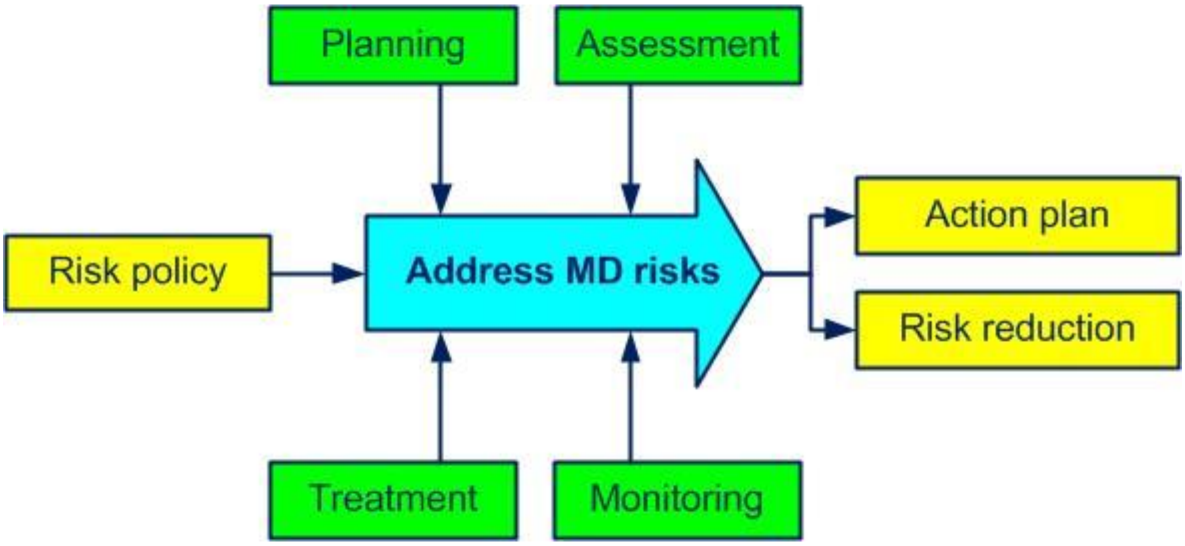


Figure 4-3. The process Address MD risks

As we will see in the following chapters, some processes include activities or sub-processes. A description of the process activities in the form of a flow diagram is shown in annex B.2, figure B.1 of ISO 14971 with details of the relevant paragraphs.

The “Address MD risks” process allows you to:

- identify the hazards and hazardous situations that may result from them
- estimate and evaluate the risks
- control risks
- monitor the effectiveness of risk control measures

A list of risks is proposed in annex 11.

A risk manager should always assume that the list of risks considered, no matter how extensive, is incomplete. Douglas Hubbard

Risk management is dynamic, iterative and responsive to any change.

The “Address MD risks” process includes the following elements:

- risk analysis, cf. clause 5
- risk evaluation, cf. clause 6
- risk management, cf. clause 7
- production and post-production activities, cf. clause 10

The MD processes are described in clause 7 of ISO 13485, cf. the T 22v16 training.

Good practices

- *the process map contains enough arrows to clearly show who the customer is (internal or external)*
- *the added value of the process is revealed during the process review*

- *the list of processes is updated*
- *the purpose of each process is clearly defined*
- *risk management requirements are respected at all stages of the MD life cycle*
- *all staff know the activities of the "Address risks" process*

Bad practices

- *some process output elements are not correctly defined (customers not taken into account)*
- *list of processes not updated*
- *non-formalized process owner*
- *very real activities are not identified in any process*
- *requirements are not met at certain phases of the MD life cycle*
- *people do not know essential activities of the "Address risks" process*

4.2 Top management responsibilities

Requirements 12 to 19

Give freedom, you will get responsibility. Reed Hastings

Top management commitment to the "Address MD risks" process consists, among other things, of ensuring the availability of the necessary resources and staff with in-depth expertise in risk management.

Top management establishes a risk policy (risk management policy), cf. annex 12 in order to:

- set risk acceptability criteria
- provide a framework guaranteeing the criteria set's compliance with applicable regulations and standards
- take into account:
  - the accepted state-of-the-art
  - the concerns, needs and wishes of stakeholders

The risk policy may include:

- the scope
- goals
- the principles
- responsibilities

The policy is updated once a year.

One possibility for the risk acceptability criteria is to choose as a risk reduction approach, without modifying the benefit-risk ratio, between as many as:

- reasonably practicable
- reasonably achievable
- possible

True story

The Manhattan military project (the creation of the atomic bomb) was moving too slowly. Secrecy was required for security reasons and the very nature of the project was hidden from all staff.

To move up a gear, project manager Robert Oppenheimer decided to inform all members of the team of the nature of the project, its extreme urgency and its crucial importance for the end of the war. An unsuspected energy was released; the work progressed by leaps and bounds.

Informing about the mission, giving meaning to the work and trusting the staff are guarantees of success for any project.

Top management and auditors regularly check the effectiveness of the “Address MD risks” process, cf. annex 13. Any decision taken or action carried out in relation to the process is documented, cf. annex 14. 🗋

When the manufacturer has implemented a quality management system, which is almost always the case, checking the effectiveness of the “Address MD risks” process is part of the management review.

Good practices

- *the risk policy takes into account all the specificities related to the corporate culture*
- *top management regularly checks the effectiveness of the “Address risks” process during the management review*
- *the job description of the risk manager includes raising staff awareness of the different requirements*

Bad practices

- *the risk policy does not take into account all the specificities related to the corporate culture*
- *the risk policy is not up-to-date*
- *the risk policy is not displayed outside the director’s office*
- *top management does not regularly check the effectiveness of the “Address risks” process*

4.3 Competence of personnel

Requirements 20 to 23

To succeed in life, you must find a domain, a skill, or something that you love to do and for which you are naturally gifted. Bob Davids

People carrying out activities linked to the “Address MD risks” process are competent thanks to their:

- education
- training
- experience
- knowledge

These people have for the use of MD:

- practical knowledge on:
  - the development of the MD
  - how does the MD work
  - how MD is made
  - how the MD is used
  - implementation of the “Address MD risks” process
- convincing experience
- control of:
  - technologies involved
  - risk management methods

Top management assigns specific responsibilities and authorities to the risk manager in relation to the “Address MD risks” process, cf. annex 15.

(Almost) true story

The story of the three stonecutters conveys a great deal. When asked about their work:

- the first replied that he is cutting stones for a living
- the second that he tries to be the best stonemason in the country
- while the third answered that he is building a cathedral

Hence the three main types of relationship to work:

- livelihood
- career
- vocation

A record of the skills required of the people involved, including experts and consultants, is kept up to date (personal files).

Minute of relaxation. Cf. the “Gold contract” joke

Good practices

- *the skills for each activity are determined in a file*
- *recruitment is consistent with top management decisions*
- *job descriptions for all positions (including executives) are accessible on the network*
- *the annual training program is updated at least twice a year*
- *the training file of each employee is protected (access restrictions)*

Bad practices

- *the annual training program is not updated (training planned but not provided)*
- *some job descriptions are non-existent*
- *missing skills are not listed*
- *evaluation of the effectiveness of training is not carried out*
- *the level of risk of training based on their impact on the safety and performance of the medical device is not identified*
- *certain training courses were not evaluated either at the end of the session or later*
- *certain skills are not determined*

4.4 Risk management plan

Requirements 24 to 35

The tiles which protect from the rain were all installed in good weather. Chinese proverb

The risk management plan is part of the risk management file, cf. § 4.5 and annex 16.

True story

The power supply to the computer room must be interrupted due to maintenance work. This is an opportunity to simulate a power outage. The staff is notified in order to observe how the shutdown of the servers will take place.

The planned day arrives: the power is cut off and the power goes to inverters, which provide around 50 minutes of autonomy. Operators initiate machine shutdown procedures in the computer room. But some machines are in a locked cabinet, which was not planned! We end up finding the bunch of keys, but they are not clearly identified, which wastes time trying them one by one. In the end, what remains is a machine that cannot be accessed: the cabinet key is found but not the second one needed to activate the keyboard. The machine ends up stopping due to lack of power, which was not planned! But it turns out that this machine is rightly considered critical.

Conclusion: a small oversight almost ruined everything! Concerning critical machines, it is better to analyze all potential problems in advance and in detail.

The plan allows, among other things, to get organized, to remain objective and not to forget any significant element.

The risk management plan includes at least:

- the scope of the MD, including the life cycle phases for each element of the plan
- the responsibilities and authorities assigned
- review of risk management activities, including those of top management
- the risk acceptability criteria for each MD, according to the acceptable risks and also when the likelihood of occurrence of harm cannot be estimated (only the severity of the harm is taken into account)
- a method for evaluating the overall residual risk, cf. clause 8
- activities to verify the implementation of risk control measures and the effectiveness of these measures
- activities to collect and review feedback from production and post-production

Annex C of ISO/TR 24971 contains, among other things, examples and recommendations on risk policy and risk acceptability criteria.

Any change to the risk management plan is recorded in the risk management file, cf. § 4.5 and annexes 16 and 25.

Good practices

- *the risk management plan includes all phases of the MD life cycle*
- *the acceptability criteria of each MD are justified*
- *changes to the risk management plan are recorded*

Bad practices

- *phases of the MD life cycle are not included in the risk management plan*
- *peripheral devices are included in the plan without reason*
- *acceptability criteria are not established*
- *no method for evaluating the overall residual risk is used*

4.5 Risk management file

Requirements 36 to 40

If it's not documented, it didn't happen. Milt Dentch

For each MD throughout its life cycle, the manufacturer establishes and maintains a risk management file, cf. annex 17.

Records included may only be referenced, but readily available, if needed.

The risk management file makes it possible to maintain traceability of each hazard identified in relation to:

- risk analysis
- risk evaluation
- the implementation and verification of the effectiveness of control measures
- the results of the residual risk evaluation

To do this, each document is indexed (or includes a version number).

Concerning medical devices that include software, the IEC 62304 standard requires traceability:

- software
- software system testing
- the risk control measure used

The risk management file includes, among other things:

- the Address risk process sheet, cf. annex 04
- the Monitor post-market process sheet, cf. annex 05
- the Evaluate benefit-risk ratio process sheet, cf. annex 07
- risk policy, cf. annex 12
- decisions and actions, cf. annex 14
- the risk management plan, cf. annex 16
- risk analysis activities, cf. annex 18
- risk evaluation activities, cf. annex 19
- control measures, cf. annex 21
- the benefit-risk ratio, cf. annex 22
- control measures review, cf. annex 23

- the completeness control review, cf. annex 24
- the accompanying documentation, cf. annex 25
- the risk management report, cf. annex 26
- the PMM (post-marketing monitoring) plan, cf. annex 27
- the PMM (post-marketing monitoring) report, cf. annex 28
- the list of collected information, cf. annex 29
- review of the collected information, cf. annex 31

Any incomplete activity in the “Address MD risks” process such as an unidentified hazard, non-evaluated risk or ineffective risk control measure can result in significant harm.

The risk management file is available to all staff.

Good practices

- *the risk management file of each MD is complete*
- *the risk management file of each MD is up-to-date*
- *the risk management file allows you to consult the traceability of identified hazards*

Bad practices

- *the risk management files of certain MDs are not complete*
- *the risk management files of certain MDs are not up-to-date*
- *the risk policy is not included in the MD risk management file*