Grant Agreement No.: 101095542
Call: HORIZON- HLTH-2022-IND-13
Topic: HORIZON-HLTH-2022-IND-13-01
Type of action: HORIZON-RIA

CYLCOMED

Cyber-security toolbox
for connected medical devices

D4.2 Risk Benefit Scheme and Risk Management Tool

Revision: v.1.0

Work package	WP 4
Task	Task 4.2
Due date	31/03/2024
Submission date	29/03/2024
Deliverable lead	INOV
Version	1.0
Authors	João Rodrigues (INOV), Gonçalo Cadete (INOV), Duarte Nascimento (INOV)
Reviewers	Pietro Di Maggio (MCI), Simone Favrin (MCI)

Abstract	This document reports the risk management tool that is being developed for the project, as well as the benefit-risk analysis methodology for evaluating the benefits and the risks of Connected Medical Devices.
Keywords	Connected Medical Devices, Risk Management Tool, Safety, Threat, Risk, Vulnerability, Benefit-Risk Analysis

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V0.1	18/03/2024	First Issue	INOV
V0.2	26/03/2024	Revision	MCI
V1.0	28/03/2024	Reviewers' comments and suggestions incorporated	INOV

Disclaimer

The information, documentation and figures available in this deliverable are written by the " Cyber security toolbox for connected medical devices" (CYLCOMED) project's consortium under EC grant agreement 101095542 and do not necessarily reflect the views of the European Commission.

The European Commission is not liable for any use that may be made of the information contained herein.

Copyright notice

Project co-funded by the European Commission in the Horizon Europe Programme	
Nature of the deliverable:	R

Dissemination Level		
PU	*Public, fully open, e.g. web*	**x**
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

* *R: Document, report (excluding the periodic and final reports)*
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.
DATA: Data sets, microdata, etc
DMP: Data management plan
ETHICS: Deliverables related to ethics issues.
SECURITY: Deliverables related to security issues
OTHER: Software, technical diagram, algorithms, models, etc.

Executive summary

Healthcare products bring benefits to patients and/or healthcare providers. Benefits can include simplified and facilitated care, symptom relief, minimal invasive interventions and the sustaining of life. Healthcare products also introduce risks. These risks can lead patients to be exposed to hazardous situations, which can impact the patient's health.

Connected Medical Devices (CMD) can be used to change the way patients are treated. When monitoring patients' vital signs in real-time, actuators could correct any identified abnormalities, enabling a better quality of life, less clinicians' interventions and better care at home. On the other hand, devices connected to the internet are subject to cybersecurity and privacy risks.

The CYLCOMED project aims to provide a methodological and technical cybersecurity framework designed for healthcare services that use CMDs. This framework will be aligned with the Medical Device Regulation (MDR) and the In Vitro Diagnostics Regulation (IVDR), but strengthens the adherence to requirements concerning safety, performance and IT security.

This document reports the status of the CYLCOMED risk management tool (first release) and the CYLCOMED benefit-risk analysis process design.

In this document, the risk management process of ISO 14971:2019 for managing medical devices is presented, with stronger focus on the risk analysis part of the process flow. A brief introduction of the benefit-risk analysis methods used in healthcare is provided, following the presentation of the developed generalized benefit-risk analysis method. Also, the first release of the CYLCOMED risk management tool is also documented.

Funded by Horizon Europe
Framework Programme of the European Union

Table of contents

Funded by Horizon Europe Framework Programme of the European Union

List of figures

Funded by Horizon Europe
Framework Programme of the European Union

List of tables

No table of figures entries found.

Funded by Horizon Europe Framework Programme of the European Union

Abbreviations

CMD	Connected Medical device
IVDR	In Vitro Diagnostics Regulation
MDR	Medical Device regulation
RMF	Risk Management Framework
SaMD	Software as a Medical Device

Funded by Horizon Europe Framework Programme of the European Union

1 Introduction

Healthcare products should bring benefits to patients and/or healthcare providers. Benefits can include simplified and facilitated care, symptom relief, minimal invasive interventions, and the sustaining of life (e.g. pacemaker) [1]. Healthcare products also introduce risks. For example, wrong dosage of insulin (e.g., due to wrong readings of blood glycaemia levels), wrong calibration of radiation levels (e.g., in a X-ray scan), or malfunctioning of a medical equipment, could pose serious threats to the patients and the surrounding personnel/environment.

When considering Connected Medical Devices, benefits in real-time monitoring of patients vital signs enable a real-time detection of abnormalities, improve clinical treatment response time, reduce hospital costs, and improve quality of care [2]. Some CMD actuators could correct the abnormality (e.g., when a blood glucose monitor alerts a high level of glucose in type II diabetes patient, an infusion pump connected to the monitor adjusts the insulin dosage and administers it automatically to the patient), enabling a better quality of life to the patient, less clinicians' interventions, and better care at home. On the other hand, devices connected to the internet are subject to cybersecurity and privacy risks.

According to the National Institute of Standards and Technology (NIST), a cybersecurity risk "relates to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflects the potential adverse impacts to organizational operations (i.e. mission functions, image, or reputation) and assets, individuals, other organizations, and the Nation“[1]. For example, the loss of integrity of information from a vital sign monitoring system can trigger undesirable responses from CMDs. A wrong blood glucose reading can lead to a wrong insulin dosage, exposing the patient to a hazardous situation of overdose or underdose.

Privacy risks, although without direct impact to patients' safety, are also of major concern. A study conducted in [3] reports impacts on patient's life such as: fear, embarrassment, emotional distress, financial strain, anxiety, blackmail, and even death (e.g., a case where an information breach indicating that an influential person in politics had an implantable cardiverter-defibrilator, led to an attacker's access and manipulation of the device, which resulted in a cardiac arrhythmia).

The CYLCOMED project aims at providing a methodological and technical cybersecurity framework designed for healthcare services that use CMDs. Such a framework is aligned with the Medical Device Regulation (MDR) and the In Vitro Diagnostics Regulation (IVDR) regulations, but strengthens the adherence to requirements concerning safety, performance and IT security. In particular, CYLCOMED will:

- Identify gaps and introduce new safety and security requirements based on evidence, adapting such requirements to novel technologies (e.g. cloud computing, artificial intelligence);
- Identify security-related hazard categories and risk acceptance criteria according to the classification of medical devices;
- Promote a risk assessment framework built on risk-benefit analyses that responds to the identified requirements and gaps and considers the impacts of novel scenarios on risks (e.g. safety, performance and environmental differences of in-hospital with respect to, remote monitoring of patients);
- Provide tools that help mitigate risks and the increase of safety, security and performance of healthcare services relying on CMD/IVD/SaMD with consideration to challenges involving legacy devices;

[1] *https://csrc.nist.gov/glossary/term/cybersecurity_risk*

Funded by Horizon Europe Framework Programme of the European Union

- Demonstrate the performance and applicability of the implemented tools in two dedicated pilots; this will provide a real-world validation performed by relevant stakeholders;
- Deliver training for end users (e.g., clinicians, patients) to increase cybersecurity awareness;
- Promote the CYLCOMED approach in the scientific community and to relevant stakeholders in the market.

The ultimate goals of the project are to:

- Improve the effectiveness and quality of personalized healthcare;
- Reduce risks and non-compliance costs.

To this end, a risk management tool for connected medical devices is being developed, as well as a benefit-risk analysis process. The objective of the risk management tool is to manage the cybersecurity, privacy and safety risks of CMDs, taking into account:

- Cybersecurity standards, such as ISO 27001;
- Privacy standards, such as the ISO 27701, which is compatible with GDPR.
- Safety standard, namely the most prominent standard used by medical device manufacturers, the ISO 14971:2019 standard, which is compatible with the MDR and the IVDR regulations;

The ISO 14971:2019 standard specifies that manufacturers are obliged to perform a benefit-risk analysis in certain conditions (explored in this report), although it does not specify a method for doing so, as there are a multitude of therapeutic areas, with very different ways of characterizing the benefits, the risks and distinct methodologies to balance / compare them. Comparing benefits and risks, establishing a way to weight them, or finding what should be the analysis data is not trivial, especially with the constant emergence of innovative therapeutics and technologies. On the other hand, there are several benefit-risk analysis schemes, developed with different scopes and objectives, within the healthcare literature. Most of them are drug development related, which can be adapted to evaluate the benefits and risks of drug administering devices. These schemes can also hint at how to evaluate benefits and risks within certain therapeutic areas, or diseases, and at how to compare the benefits and risks among conventional treatments versus treatments with CMDs.

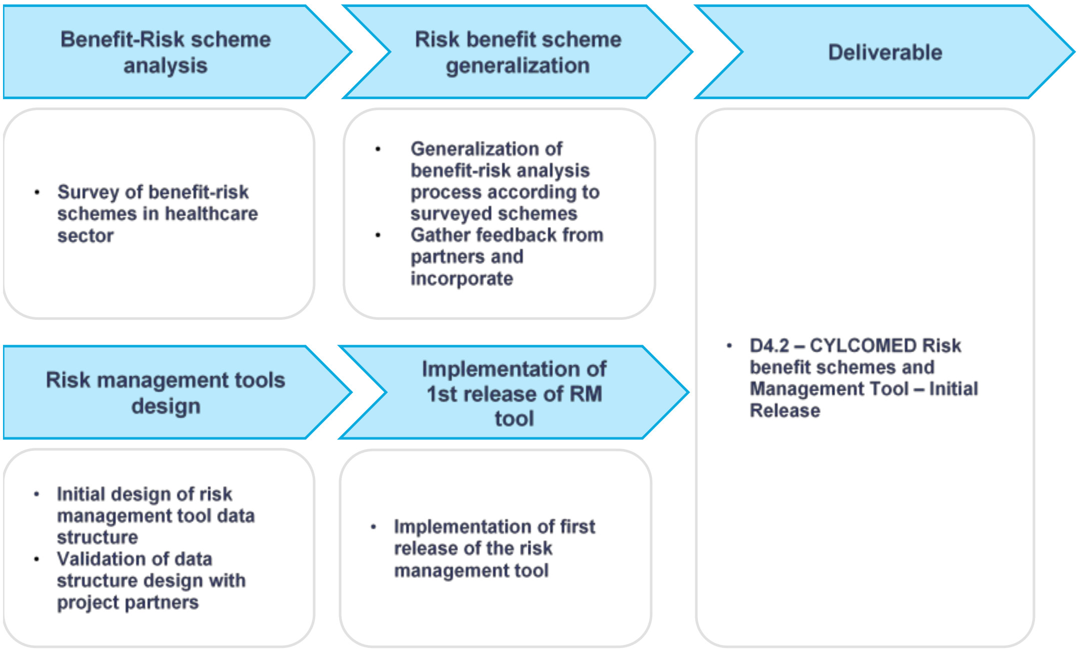
This report focuses on the status of the risk management tool and the CYLCOMED benefit-risk analysis process.

1.1 Methodology

To elaborate this report, the following methodology was followed:

- First, an extensive survey was carried out to determine the benefit-risk schemes that were used within the healthcare sector.
- At the same time, the initial design of the risk management tool, building from previous study on risk management frameworks. Once the data model was designed, it was shared among the consortium, changed taking into account the partners feedback, and finally validated for the first release.
- Then, a generalization of the benefit-risk schemes was carried out, and the result was shared and validated by the consortium for the first release. The first release of the risk management tool was developed.
- Finally, this report was prepared.

Funded by Horizon Europe Framework Programme of the European Union


Benefit-Risk scheme analysis

- Survey of benefit-risk schemes in healthcare sector

Risk benefit scheme generalization

- Generalization of benefit-risk analysis process according to surveyed schemes
- Gather feedback from partners and incorporate

Deliverable

- D4.2 – CYLCOMED Risk benefit schemes and Management Tool – Initial Release

Risk management tools design

- Initial design of risk management tool data structure
- Validation of data structure design with project partners

Implementation of 1st release of RM tool

- Implementation of first release of the risk management tool

Figure 1 Methodology for elaboration of this report

1.2 Structure of the document

This report is structured as follows:

- Section 2 is dedicated to the risk management process of ISO 14971:2019 for managing medical devices, with stronger focus on the risk analysis part of the process flow;
- Section 3 gives a brief introduction into benefit-risk analysis methods;
- Section 4 describes the developed generalized benefit-risk analysis method;
- Section 5 presents the first release of the CYLCOMED risk management tool;
- The final section is reserved for the conclusions.

Funded by Horizon Europe Framework Programme of the European Union

2 Risk management of medical devices

2.1 Manufacturer’s perspective

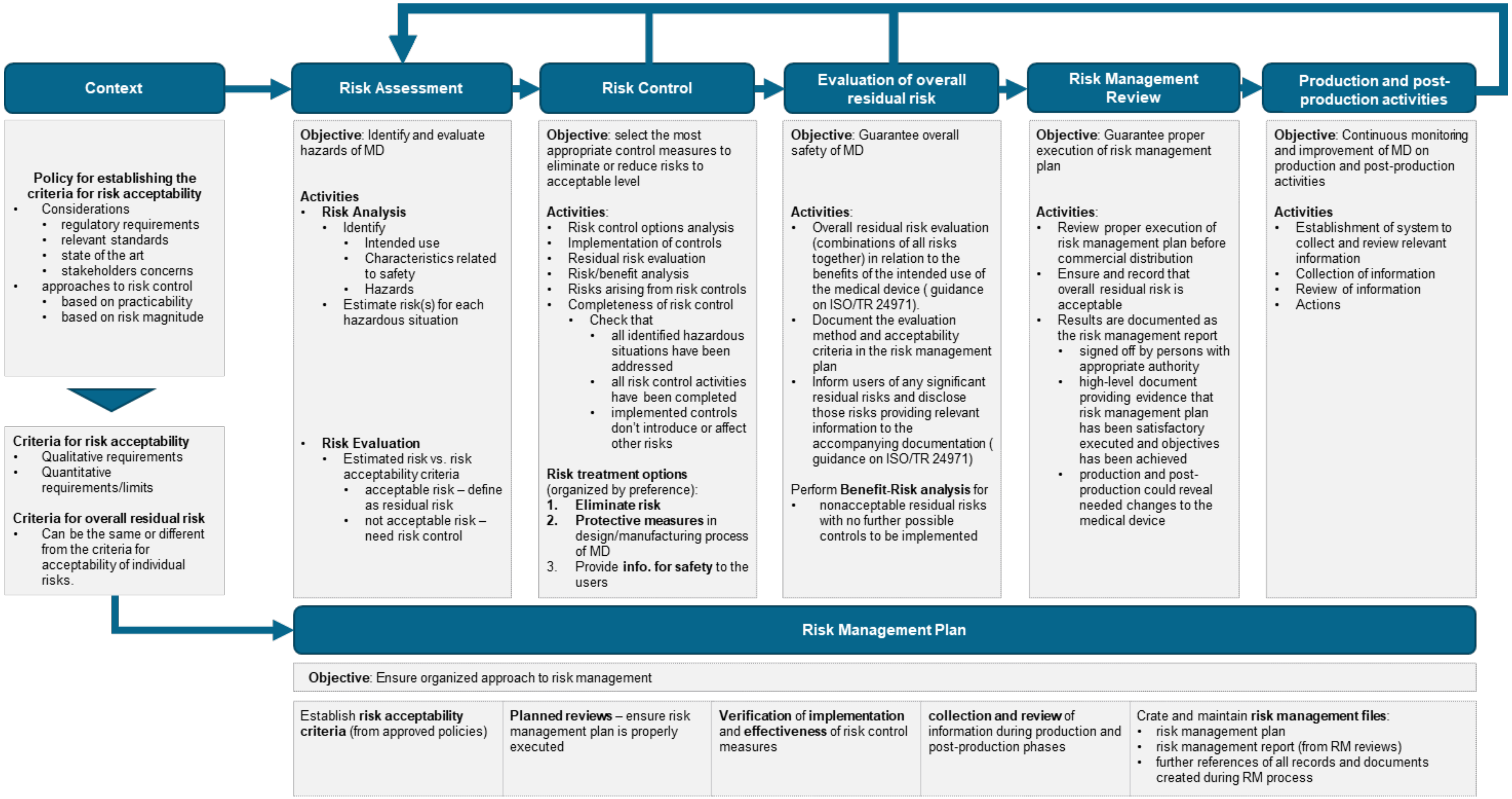
ISO 14971 is a risk management standard for manufacturers of medical devices [4] [5]. It describes the process by which manufacturers can manage the risks of their MD throughout its life cycle. It outlines how to structure the risk management process and what activities should be performed to guarantee MD safety for medical use.

According to the International Organization for Standardization (ISO), the European standard EN ISO 14971:2019, together with amendment A11:2021, Annexes Z addresses the coverage of the MDR and IVDR regulations by the standard [4], [6].

The Risk Management process described in ISO 14971 and depicted in Figure 2 has six stages:

- Risk Management Plan;
- Risk Assessment;
- Risk Control;
- Evaluation of overall residual risk;
- Risk Management Review;
- Production and post-production activities.

Funded by Horizon Europe Framework Programme of the European Union



Context

Policy for establishing the criteria for risk acceptability

- Considerations
  - regulatory requirements
  - relevant standards
  - state of the art
  - stakeholders concerns
- approaches to risk control
  - based on practicability
  - based on risk magnitude

Criteria for risk acceptability

- Qualitative requirements
- Quantitative requirements/limits

Criteria for overall residual risk

- Can be the same or different from the criteria for acceptability of individual risks.

Risk Assessment

Objective: Identify and evaluate hazards of MD

Activities

- **Risk Analysis**
  - Identify
    - Intended use
    - Characteristics related to safety
    - Hazards
  - Estimate risk(s) for each hazardous situation
- **Risk Evaluation**
  - Estimated risk vs. risk acceptability criteria
    - acceptable risk – define as residual risk
    - not acceptable risk – need risk control

Risk Control

Objective: select the most appropriate control measures to eliminate or reduce risks to acceptable level

Activities:

- Risk control options analysis
- Implementation of controls
- Residual risk evaluation
- Risk/benefit analysis
- Risks arising from risk controls
- Completeness of risk control
  - Check that
    - all identified hazardous situations have been addressed
    - all risk control activities have been completed
    - implemented controls don't introduce or affect other risks

Risk treatment options (organized by preference):

1. **Eliminate risk**
2. **Protective measures** in design/manufacturing process of MD
3. Provide **info. for safety** to the users

Evaluation of overall residual risk

Objective: Guarantee overall safety of MD

Activities:

- Overall residual risk evaluation (combinations of all risks together) in relation to the benefits of the intended use of the medical device (guidance on ISO/TR 24971).
- Document the evaluation method and acceptability criteria in the risk management plan
- Inform users of any significant residual risks and disclose those risks providing relevant information to the accompanying documentation (guidance on ISO/TR 24971)

Perform **Benefit-Risk analysis** for

- nonacceptable residual risks with no further possible controls to be implemented

Risk Management Review

Objective: Guarantee proper execution of risk management plan

Activities:

- Review proper execution of risk management plan before commercial distribution
- Ensure and record that overall residual risk is acceptable
- Results are documented as the risk management report
  - signed off by persons with appropriate authority
  - high-level document providing evidence that risk management plan has been satisfactory executed and objectives has been achieved
  - production and post-production could reveal needed changes to the medical device

Production and post-production activities

Objective: Continuous monitoring and improvement of MD on production and post-production activities

Activities

- Establishment of system to collect and review relevant information
- Collection of information
- Review of information
- Actions

Risk Management Plan

Objective: Ensure organized approach to risk management

Establish **risk acceptability criteria** (from approved policies)

Planned reviews – ensure risk management plan is properly executed

Verification of **implementation** and **effectiveness** of risk control measures

collection and review of information during production and post-production phases

Crate and maintain **risk management files**:

- risk management plan
- risk management report (from RM reviews)
- further references of all records and documents created during RM process

Figure 2 ISO 14971 Risk management process

Funded by Horizon Europe Framework Programme of the European Union

2.1.1 Context

Before starting the risk management process, a policy document detailing how to establish the risk acceptability criteria for the medical device must be written. Applicable regulations, standards, state of the art and stakeholders' perspectives and concerns are among the topics that should be covered. This policy should be a framework for establishing risk acceptability criteria for every medical device the manufacturer produces.

The risk acceptability criteria are tailored for a specific medical device and its purpose, and it can be composed of quantitative and/or qualitative requirements. The criteria must be established for individual risks and for residual risks.

2.1.2 Risk Management Plan

In the Risk Management Plan stage, the roadmap for risk management is defined and maintained. It is in this stage that the risk acceptability criteria are defined, as well as all the activities for monitoring, reviewing and acting on the risk management process, from MD conception to post-production. In this stage, risk management files must be created and should include the risk management plan, risk management reports and references to other relevant records and documents created during the risk management process.

2.1.3 Risk Assessment

The risk assessment stage has two sets of activities: risk analysis and risk evaluation.

In the risk analysis activities, the use and misuse of the MD (in relation to the objectives for which the MD was designed by the manufacturer); the safety characteristics of the MD (i.e., how the MD affects the safety of devices); and the hazards of using the MD (i.e., potential sources of harm), are identified.

Then, the risks are estimated for each hazardous situation. In the risk evaluation activities, for each identified risk both probability and severity of the risk are assessed. Then each identified risk is evaluated against the risk acceptability criteria defined in the risk management plan. Acceptable risks are deemed residual risk and the risks that are not acceptable will need risk control measures. All risk assessment process activities, used methodologies and results should be documented in the risk management file.

Use and Misuse of the MD

The relation between the use and misuse of the MD is depicted in Figure 3.

The intended use of the MD is the use for which the MD was designed by the manufacturer. Typical elements of the intended use include the intended medical indication, patient population, user profile, environment, etc. Along with the intended use, other uses of the MD like maintenance of the device, calibration, transportation conditions, are defined as well. The intended use and other use define the correct use of the MD, which is also defined as reasonably foreseeable use.

Sometimes, even when following all indications for the correct use of the MD, some errors can occur due to lapses or mistakes in the use of the MD. This is defined as use error.

The user intent plays a role on the classification of MD use. If the user intends to use the MD correctly, following the prescribed instructions, or the generally accepted practice for the MD, then, this user either uses the MD correctly or with error. The correct use and the use error constitute what is defined as normal use.

A user can purposely use the MD without following the prescribed instructions, or the generally accepted practice. In this case, user actions can be predictable or unpredictable. The

Funded by Horizon Europe Framework Programme of the European Union

predictable actions are defined as foreseeable user behaviour, and the unpredictable actions are defined as unforseeable user behaviour.

The use error and foreseeable user behaviour define the reasonably foreseeable misuse. The unforeseeable user behaviour falls under the category of not reasonably foreseeable misuse. These uses are not intended by the manufacture.

2.1.4 Risk Control

In the risk control stage, the manufacturer analyses the risk control options for each identified risk. These options should be sought out on internationally known standards, best practices and other relevant references.

The risk treatment options follow a hierarchy of preferences:

- First, it should preferably eliminate the risk;
- Second, if eliminating the risk is not possible, then protective measures in the design of and manufacturing process of the MD must be selected;
- If protective measures are not implementable, then the manufacturer must provide users with information for safety.

The selected controls must be implemented, and a new risk assessment must be performed. (see Figure 2). The processes of risk analysis and risk control measures implementation goes on as long as there are still risks that are not acceptable and there exists control measures that can be implemented. Once we arrive at a stage where there are still risks with no practical controls to be implemented, the manufacturer has three options: perform a risk-benefit analysis, restrict the intended use or modify the medical device [4]. Otherwise, the MD should not be further developed and commercialized.

All these activities must be documented in the risk management file.

2.1.5 Evaluation of overall residual risk

In the Evaluation of Overall Residual Risk stage, the residual risks are evaluated in combination with each other. This is crucial since the combination of these risks can give rise to a set of risks that are not acceptable by the risk acceptability criteria. For this evaluation, the ISO/TR 27971 provides guidance on evaluating these risks and informing users when needed. The evaluation method, the used acceptability criteria and the performed analysis must be documented in the risk management file.

2.1.6 Risk Management Review

The Risk Management Review stage concerns with controlling the proper execution of the risk management plan before commercial distribution of the MD. It guarantees that all records concerning residual risks exists, are properly performed and that every residual risk is acceptable. These controls are done in the form of reviews and they are documented in risk

Funded by Horizon Europe Framework Programme of the European Union

management reports which obliges the clearance/acceptance of a person with the due authority within the manufacturer’s organization.

2.1.7 Production and Post-Production Activities

In the Production and Post-Production Activities stage, a system for collecting and reviewing relevant information of the MD on production and post-production phases must be established. The collected and reviewed information must trigger any corrective actions on the MD’s life cycle if new risks/hazards are discovered.

Funded by Horizon Europe
Framework Programme of the European Union

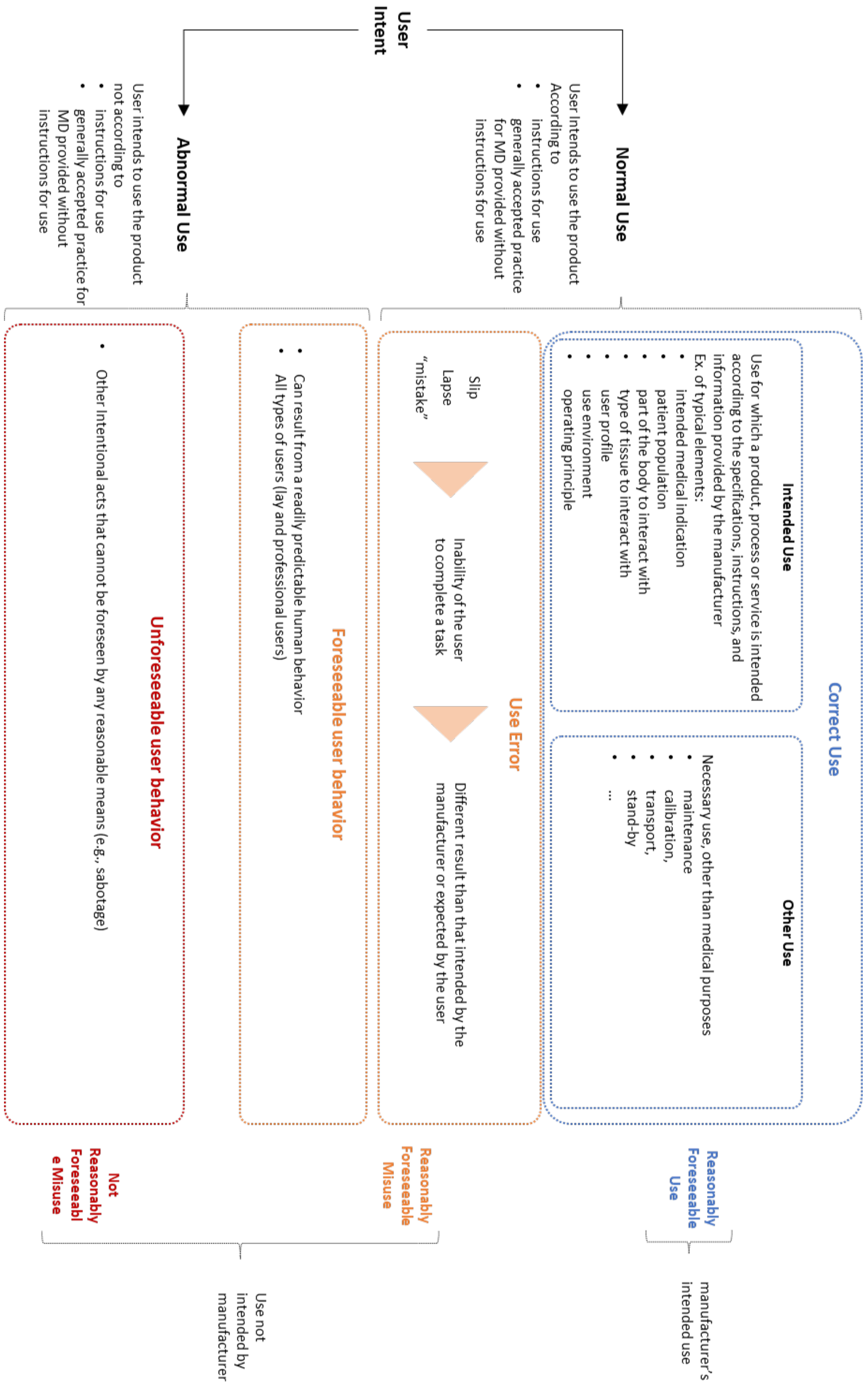

User Intent
Normal Use
User Intends to use the product According to
• instructions for use
• generally accepted practice for MD provided without instructions for use
Abnormal Use
User intends to use the product not according to
• instructions for use
• generally accepted practice for MD provided without instructions for use
Correct Use
Intended Use
Use for which a product, process or service is intended according to the specifications, instructions, and information provided by the manufacturer
Ex. of typical elements:
• intended medical indication
• patient population
• part of the body to interact with
• type of tissue to interact with
• user profile
• use environment
• operating principle
Other Use
• Necessary use, other than medical purposes
• maintenance
• calibration,
• transport,
• stand-by
• ...
Use Error
Slip
Lapse
"mistake"
Inability of the user to complete a task
Different result than that intended by the manufacturer or expected by the user
Foreseeable user behavior
• Can result from a readily predictable human behavior
• All types of users (lay and professional users)
Unforeseeable user behavior
• Other Intentional acts that cannot be foreseen by any reasonable means (e.g., sabotage)
Reasonably Foreseeable Use
Reasonably Foreseeable Misuse
Not Reasonably Foreseeabl e Misuse
manufacturer's intended use
Use not intended by manufacturer

Figure 3 Relation between the use and misuse of the medical device adapted from [4] and [7]

Funded by Horizon Europe Framework Programme of the European Union

2.2 Evaluation of hazardous situations

When evaluating the risks of the medical device, the manufacturer must:

- Derive the possible hazardous situations when using the medical device, from the intended use and from the reasonably foreseeable misuse;
- Perform the risk analysis of the harms that a hazardous situation can lead to.

As defined in [8]:

- a hazard is defined as a "potential source of harm";
- a hazardous situation is defined as "a circumstance in which people, property or the environment is/are exposed to one or more hazards";
- harm is defined as "injury or damage to the health of people, or damage to property or the environment".

Hazards can be of various types, such as [9]:

- Energy hazards, including acoustic, electric, mechanical, potential, radiation and thermal energies;
- Biological and chemical hazards, including biological agents, chemical agents and immunological agents;
- Performance-related hazards, coming from data storage and handling, the delivery of the treatment, diagnostic information and functionality.

The process of identification of hazards and related risk analysis is depicted in Figure 4.

From the intended use, the manufacturer should consider safety characteristics such as the following:

- MD usage (e.g. aim, population, diagnosis, prevention of condition, contact with patient, etc);
- Components/materials of the MD;
- Energy transferred to patient (radiation, vibration);
- Substance delivered/extracted to/from patients;
- Microbiological control/sterilization;
- Environment modification (temperature, humidity, toxic materials, etc);
- Measurements (e.g. vital signs, accuracy, precision, data);
- Data/sample interpretation (e.g. software, AI, ML, etc);
- Use with other MDs/technologies;
- Undesirable outputs (radiation, noise, chemicals, etc);
- Environmental influence (operation, transport, storage);
- Consumables or accessories (e.g., syringes);
- Maintenance/calibration;
- Software/access to information/data;
- Shelf life;
- Long-term use effects;
- Mechanical forces (from/to MD);
- Lifetime of MD;
- Single use considerations (if applicable);

Funded by Horizon Europe Framework Programme of the European Union

- Decommission/disposal;
- Special training to use/install MD;
- Safety information availability;
- Manufacturing processes;
- User interface – usability – how it affects effectiveness of MD;
- Alarm system(s);
- Mobile/portable MD considerations if applicable;
- Essential performance needs;
- MD autonomy features considerations;
- Considerations for output data for clinical action;
- Misuse considerations.

Next, based on the safety characteristics, the hazards are identified. The cybersecurity and privacy risks fall under the performance-related hazards described above. Data access, availability, confidentiality, integrity and transferring, delivery rate and quantity, diagnostic information properties, and functionality properties such as alarms and performance can all impact the patient safety as well as the safety of other people surrounding the device. These hazards could also affect other devices and infrastructures, as well as lead to privacy breaches.

Next, for each identified hazard, a risk analysis is performed:

- The set of events that must occur before leading to a hazard has to be identified. The probability P_i of each of these events (event i) occurring is estimated. The probability of these events leading to the hazard is the multiplication of the probability of the events occurring, $P_{HZ} = \Pi_i P_i$ (we are considering that the events are independent among themselves). Also, the circumstances affecting the severity of the hazard is evaluated.
- Then, the events leading to exposure to the hazard is determined as well, in the same manner as before, yielding the probability of occurring a hazardous situation $P_{HS} = \Pi_j P_j$, as well as the circumstances affecting the severity.
- Finally, the events leading to potential harm is determined, along with their probabilities of occurrence P_k and the circumstances affecting the severity.

The overall probability of a potential harm to occur is determined to be $P_H = P_{HZ} \times P_{HS} \times \Pi_k P_k$ and the severity level is also determined, based on the determined circumstances affecting severity.

Finally, the risk level is determined based on the probability of occurrence of the potential harm and the severity level, $r(P_H, S)$.

Funded by Horizon Europe Framework Programme of the European Union

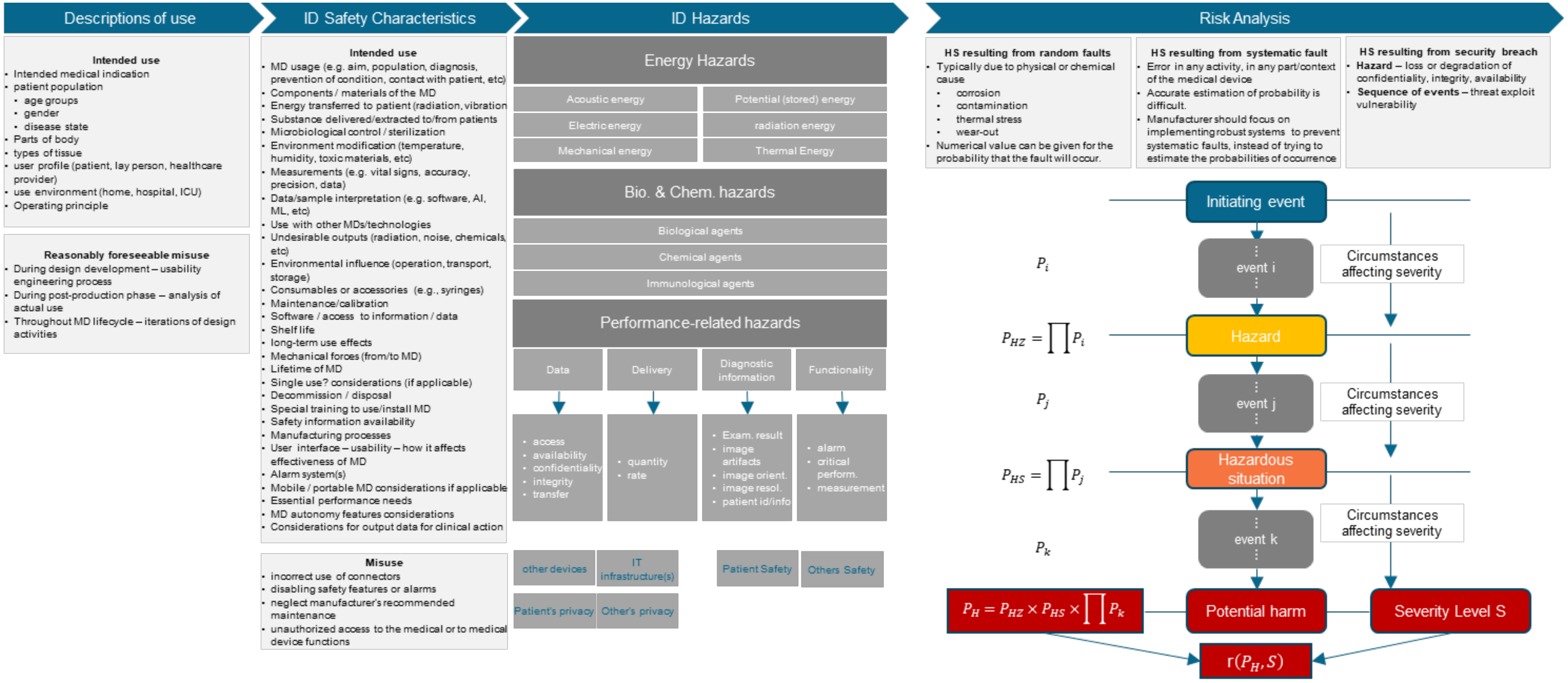

Descriptions of use
Intended use
• Intended medical indication
• patient population
• age groups
• gender
• disease state
• Parts of body
• types of tissue
• user profile (patient, lay person, healthcare provider)
• use environment (home, hospital, ICU)
• Operating principle
Reasonably foreseeable misuse
• During design development – usability engineering process
• During post-production phase – analysis of actual use
• Throughout MD lifecycle – iterations of design activities
ID Safety Characteristics
Intended use
• MD usage (e.g. aim, population, diagnosis, prevention of condition, contact with patient, etc)
• Components / materials of the MD
• Energy transferred to patient (radiation, vibration
• Substance delivered/extracted to/from patients
• Microbiological control / sterilization
• Environment modification (temperature, humidity, toxic materials, etc)
• Measurements (e.g. vital signs, accuracy, precision, data)
• Data/sample interpretation (e.g. software, AI, ML, etc)
• Use with other MDs/technologies
• Undesirable outputs (radiation, noise, chemicals, etc)
• Environmental influence (operation, transport, storage)
• Consumables or accessories (e.g., syringes)
• Maintenance/calibration
• Software / access to information / data
• Shelf life
• long-term use effects
• Mechanical forces (from/to MD)
• Lifetime of MD
• Single use? considerations (if applicable)
• Decommission / disposal
• Special training to use/install MD
• Safety information availability
• Manufacturing processes
• User interface – usability – how it affects effectiveness of MD
• Alarm system(s)
• Mobile / portable MD considerations if applicable
• Essential performance needs
• MD autonomy features considerations
• Considerations for output data for clinical action
Misuse
• incorrect use of connectors
• disabling safety features or alarms
• neglect manufacturer's recommended maintenance
• unauthorized access to the medical or to medical device functions
ID Hazards
Energy Hazards
Acoustic energy
Potential (stored) energy
Electric energy
radiation energy
Mechanical energy
Thermal Energy
Bio. & Chem. hazards
Biological agents
Chemical agents
Immunological agents
Performance-related hazards
Data
Delivery
Diagnostic information
Functionality
• access
• availability
• confidentiality
• integrity
• transfer
• quantity
• rate
• Exam. result
• image artifacts
• image orient.
• image resol.
• patient id/info
• alarm
• critical perform.
• measurement
other devices
IT infrastructure(s)
Patient's privacy
Other's privacy
Patient Safety
Others Safety
Risk Analysis
HS resulting from random faults
• Typically due to physical or chemical cause
• corrosion
• contamination
• thermal stress
• wear-out
• Numerical value can be given for the probability that the fault will occur.
HS resulting from systematic fault
• Error in any activity, in any part/context of the medical device
• Accurate estimation of probability is difficult.
• Manufacturer should focus on implementing robust systems to prevent systematic faults, instead of trying to estimate the probabilities of occurrence
HS resulting from security breach
• Hazard – loss or degradation of confidentiality, integrity, availability
• Sequence of events – threat exploit vulnerability
Initiating event
P_i
event i
Circumstances affecting severity
$P_{HZ} = \prod P_i$
Hazard
P_j
event j
Circumstances affecting severity
$P_{HS} = \prod P_j$
Hazardous situation
P_k
event k
Circumstances affecting severity
$P_H = P_{HZ} \times P_{HS} \times \prod P_k$
Potential harm
Severity Level S
$r(P_H, S)$

Figure 4 Process of identification of hazards and related risk analysis

Funded by Horizon Europe Framework Programme of the European Union

2.3 Benefit-risk evaluation process

The benefit-risk evaluation process occurs during the residual risk analysis phase, and only for those residual risks that are deemed unacceptable, as depicted in Figure 5. ISO 14971 and 24971 don't specify how to perform this analysis, as it depends on several factors like therapeutic area, technologies used, population, intended use, etc. non-the-less, some considerations for the benefits estimation are indicated, like expected performance, expected clinical outcome, similar medical devices, factors from other diagnosis/treatment options. The documents also mention the obligation of informing the users about the benefit-risk evaluation, and including it in the user documentation (e.g. user manuals). Other informed aspects include the expected benefits, the probability of the benefit materializing, the magnitude of the expected benefits and the duration of the beneficial effects.

Funded by Horizon Europe Framework Programme of the European Union

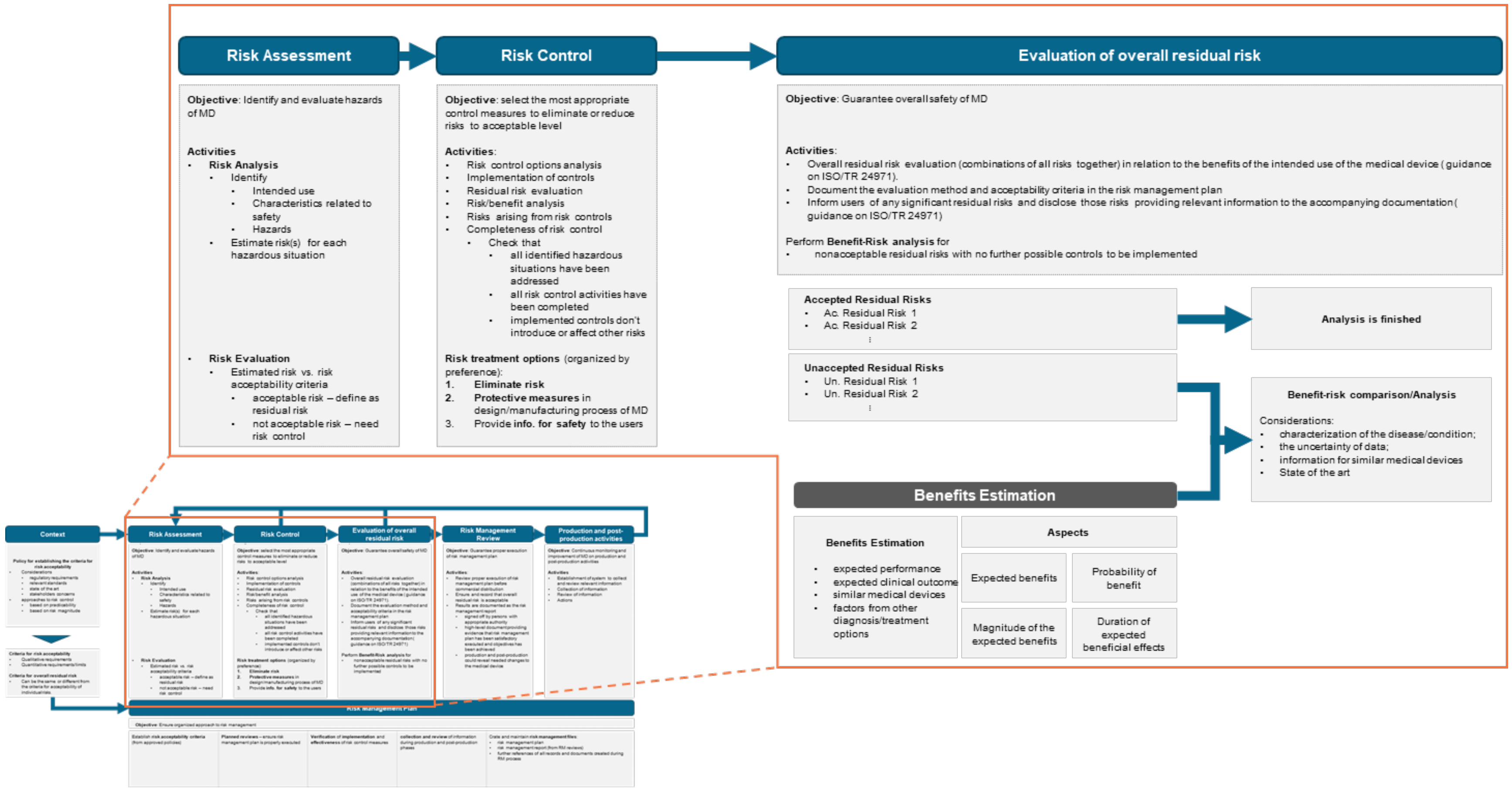

Context
Risk Assessment
Risk Control
Evaluation of overall residual risk
Risk Management Review
Production and post-production activities
Risk Management Plan
Risk Assessment
Objective: Identify and evaluate hazards of MD
Activities
Risk Analysis
Identify
Intended use
Characteristics related to safety
Hazards
Estimate risk(s) for each hazardous situation
Risk Evaluation
Estimated risk vs. risk acceptability criteria
acceptable risk – define as residual risk
not acceptable risk – need risk control
Risk Control
Objective: select the most appropriate control measures to eliminate or reduce risks to acceptable level
Activities:
Risk control options analysis
Implementation of controls
Residual risk evaluation
Risk/benefit analysis
Risks arising from risk controls
Completeness of risk control
Check that
all identified hazardous situations have been addressed
all risk control activities have been completed
implemented controls don't introduce or affect other risks
Risk treatment options (organized by preference):
1. Eliminate risk
2. Protective measures in design/manufacturing process of MD
3. Provide info. for safety to the users
Evaluation of overall residual risk
Objective: Guarantee overall safety of MD
Activities:
Overall residual risk evaluation (combinations of all risks together) in relation to the benefits of the intended use of the medical device (guidance on ISO/TR 24971).
Document the evaluation method and acceptability criteria in the risk management plan
Inform users of any significant residual risks and disclose those risks providing relevant information to the accompanying documentation(guidance on ISO/TR 24971)
Perform Benefit-Risk analysis for
nonacceptable residual risks with no further possible controls to be implemented
Accepted Residual Risks
Ac. Residual Risk 1
Ac. Residual Risk 2
Analysis is finished
Unaccepted Residual Risks
Un. Residual Risk 1
Un. Residual Risk 2
Benefit-risk comparison/Analysis
Considerations:
characterization of the disease/condition;
the uncertainty of data;
information for similar medical devices
State of the art
Benefits Estimation
Benefits Estimation
expected performance
expected clinical outcome
similar medical devices
factors from other diagnosis/treatment options
Aspects
Expected benefits
Probability of benefit
Magnitude of the expected benefits
Duration of expected beneficial effects

Figure 5 Benefit-Risk evaluation process

Funded by Horizon Europe Framework Programme of the European Union

3 Benefit-risk schemes in healthcare

Within the healthcare sector, several benefit-risk analysis schemes were developed for drugs and other medical products. Due to the quantity of such schemes, we focussed on studies that analysed several benefit-risk schemes in order to understand common patterns among them.

According to [10] and [11], the entities involved in the benefit-risk schemes are the following:

- **Patient**: the person subject to the treatment;
- **Healthcare providers/physicians**: the people who need to consider the benefits and risks of the various therapeutic options for the patients;
- **Regulators**: make decisions about benefits and risks of treatments on the basis of [10]:
  - Clinical trials before authorizing the treatment for the general public;
  - Licensing review;
  - Continuous monitoring of the treatment and benefit-risk weighting, activating the necessary means to guarantee patient safety when needed (e.g, recall treatment product, guarantee that new safety information available to the patients).
- **Manufacturer/pharmaceutical companies**: provide the medical product and constantly perform the benefit-risk assessment on the entire life-cycle of the product to update the risk mitigation activities, as well as communicate with the appropriate entities, such as regulators, healthcare insurance companies and physicians.

To define the benefit-risk scheme to be used for a medical product, the manufacturer/pharmaceutical company should have a cross functional team responsible for defining how the data required to perform the analysis will be collected. The same team is also responsible for the execution of the benefit-risk analysis process.

When it comes to benefit-risk analysis for drugs, the needed data can be obtained by (non-exhaustive list):

- **Clinical trials** – a research study of a patient population to answer specific questions of medical interest through intervention [10];
- **Observational studies** – a study in which no intervention is made (in contrast with an experimental study). Such studies provide estimates and examine associations of events in their natural settings without recourse to experimental intervention [12], [10];
- **Pharmacoepidemiological healthcare databases** – databases with data regarding effects of drugs in well-defined populations.

Comparing benefits and risks, establishing a way to weight them, or even finding what should be the analysis data is not trivial, especially with inovative therapeutics and technologies. On the other hand, there are several benefit-risk analysis schemes, developed with different scopes and objectives, described within the healthcare literature. Most of them are drug development related, but can be adapted to evaluate the benefits and risks of drug administering devices. These schemes can also hint at how to evaluate the benefits and risks within certain therapeutic areas, diseases, and at how to compare the benefits and risks among conventional treatments versus treatments with CMDs.

In [10] systematization of existing benefit-risk schemes for evaluating drugs were made. This study organized the existing benefit-risk schemes until the time of the project, as follows:

- **Descriptive frameworks**, which provide guidance for a qualitative benefit-risk evaluation process;
- **Quantitative framework**, which provide guidance for a quantitative benefit-risk evaluation process;

Funded by Horizon Europe Framework Programme of the European Union

- **Threshold indices**, based on quantitative measurements of risk benefit;
- **Health Indices**, which are quantitative measurements of risk and benefit, explicitly developed in various health contexts;
- **Trade-off indices**, which measure the trade-offs between risks and benefits, quantitatively;
- **Estimation Techniques**, which ranges from the very simple to cutting-edge statistical methods to synthetize complex data from multiple sources;
- **Utility Survey Techniques**, which complements the aforementioned approaches with preferences of various outcomes from relevant stakeholders.

For more information about the benefit-risk methods mentioned in Figure 6 a reading of [10] and the references therein is encouraged.

Funded by Horizon Europe
Framework Programme of the European Union

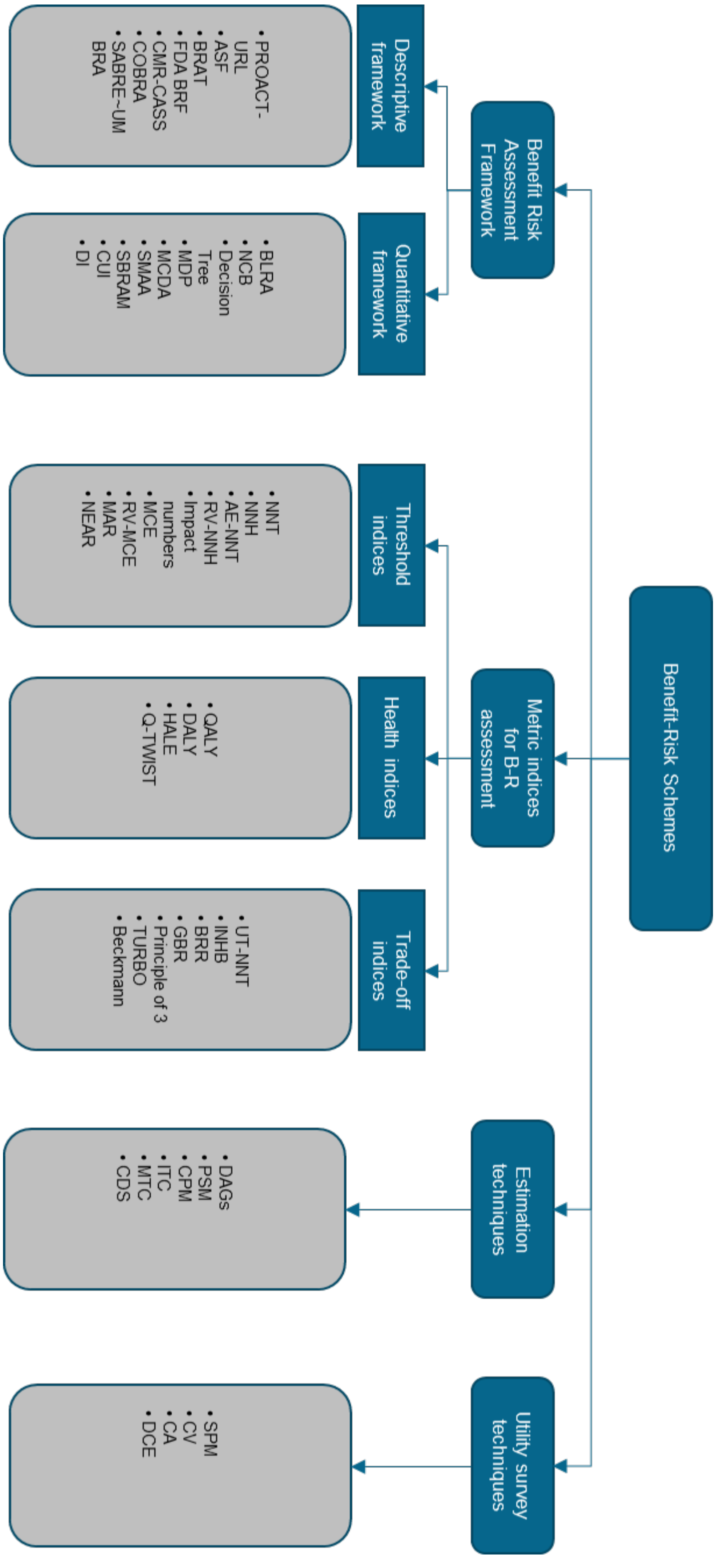


Figure 6 Systematization of existing benefit-risk schemes for evaluating drugs according to [10]

Funded by Horizon Europe Framework Programme of the European Union

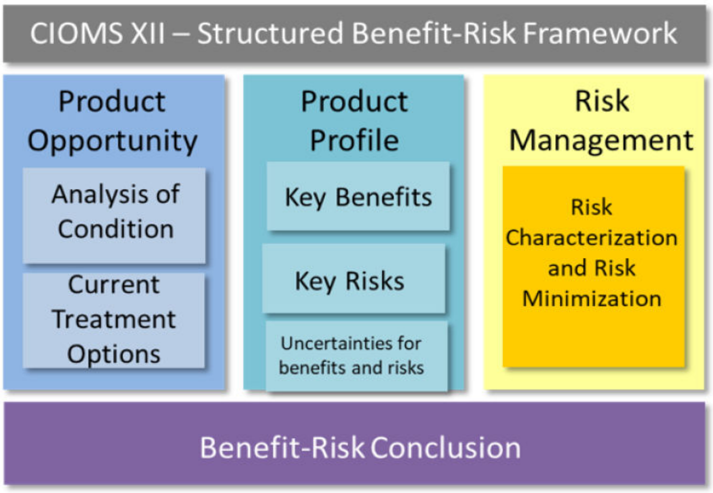

CIOMS XII – Structured Benefit-Risk Framework
Product Opportunity
Analysis of Condition
Current Treatment Options
Product Profile
Key Benefits
Key Risks
Uncertainties for benefits and risks
Risk Management
Risk Characterization and Risk Minimization
Benefit-Risk Conclusion

Figure 7 Components of the Structured Benefit-Risk Framework, adapted from [11]

In [11], a Structured Benefit-Risk approach/framework was presented (Figure 7).

This framework has 4 components:

- **Product Opportunity**, which comprises the analysis of the therapeutic area of the medical product, the condition or disease the medical product is intended to treat, and currently available treatment for the condition.
- **Product Profile**, where considerations and definitions for the benefits and risks of the product are analyzed, yielding the key benefits, the key risks, their evaluation and data acquisition methods and the uncertainties regarding, the appropriateness (or clinical relevance) of the key benefits and risks, the limitations of clinical studies processes (e.g., clinical trials patients benefit versus benefits to population in general), limits in scientific understanding and the evaluation method.
- **Risk Management,** which comprises activities for risk characterization and risk minimization with regards to the product for guaranteeing appropriate benefit-risk balance.
- **Benefit-Risk Conclusion,** which includes all the reasoning behind the first three components, and the final conclusion about whether the overall benefit-risk balance is favorable or not.

Funded by Horizon Europe Framework Programme of the European Union

4 General-purpose benefit-risk scheme

There is a wide heterogeneity of therapeutic areas, each with its way of analyzing hazards, benefits, risks and harms. As seen in the previous chapter, there exists a plethora of benefit-risk schemes for analyzing medical products, and the benefit-risk schemes for medical devices are also not prescriptive, leaving the onus of defining the analysis method to the manufacturer. Hence, based on the analysis of the benefit-risk schemes described in [10], the descriptions in [11], and the requirements of ISO/TIR 14971, a general-purpose benefit-risk scheme was developed for the CYLCOMED project, to enable a common framework for evaluating different therapeutic areas and types of medical devices, as depicted in Figure 8.

Therapeutic Context

During the therapeutic context definition, an analysis of the condition/disease is made. This analysis comprises the analysis of the nature of the disease, severity of the condition, unmet medical need and the intended population. Afterwards, current treatment options are surveyed. These analyses will promote a better understanding of the scope of the medical product and how it can be compared to other similar or complementary products in the market.

Also important are the applicable regulations, standards and laws, where compliance requirements for the medical product should be derived from as well.

Next, the key benefits and risks should be defined. For new and innovative therapeutics or technologies, the performed analysis of condition, should shed some lights on how to determine what benefits and risks should be taken into considerations. From the available treatments within the same therapeutic area, for example, or similar medical devices, it should be possible to determine the best benefits and risks considerations for benchmarking purposes. The key benefits and key risks can be organized by categories.

Evaluation Criteria

The evaluation criteria refer to the factors that should be considered when analysing the key benefits and key risks and how they should be evaluated individually. For example, when considering performance requirements like radiation levels of an RX scan device or battery life for a pacemaker, this can be analysed quantitatively, hence a quantitative evaluation criterion can be defined. Qualitative evaluation criteria can be derived from expert opinions regarding, for example, the benefits of using a medical device to patient's health (e.g. the use of the pacemaker will prevent a stroke; the use of a glycaemia monitoring system connected to the internet will enable the real-time analysis and control of diabetes patients glycemia level, yielding a better quality of life).

Comparison weights/Functions

Direct comparison between the key benefits and key risks of a medical product is usually not trivial as their evaluation criteria can be evaluated quantitatively, qualitatively, or with a mixture of both quantitative and qualitative criteria, and the factors can vary as well.

In combining different key benefits and key risks, to encompass all possible cases, we will consider the comparison weights as a particular multiplicative functions. To be general, these functions can represent a mathematical function with any dimension; or an expert analysis process that will output several impact values for each factor; a combination of factors; description; or any other parameter deemed appropriate.

In Figure 7 and Figure 8 the $b_{i,j}$ $(r_{k,l})$ represent the first transformation/agglomeration of the evaluation criteria for a specific key benefit (risk). Depending on the context, the subsequent functions $B_{i,j}, \dots, B$, $R_{k,l}, \dots, R$ and $EVAL$ can be defined to enable the comparison of any key risk and any key benefit combination.

Funded by Horizon Europe Framework Programme of the European Union

Data Acquisition

For the data acquisition process, it is crucial to have defined the evaluation data and data acquisition processes for the key benefits and risks. For example, considering an RX scan machine, the radiation levels emitted must be determined, and the data acquisition process includes the detection gears, their disposition, the physical place where the RX machine will be emitting the radiation, personnel involved, etc. These data can also include patient satisfaction or any other feedback he can provide.

These data will be used by the comparison functions, and ultimately, by the evaluation function.

Benefit-Risk Evaluation

The benefit-risk evaluation will be the result of the evaluation function applied on the comparison functions and the acquired data, and further expert analysis may be required in order to interpret the result, and also to formally document the results. This is crucial since, there exists a variety of uncertainties in the whole evaluation process as we will see next.

Sources of Uncertainties

When performing a benefit-risk evaluation, there are uncertainty areas that must be considered. In all 5 stages of the benefit-risk scheme, the uncertainty analysis must be performed by a multidisciplinary group of experts in order to better understand how they can influence the benefit-risk analysis and, ultimately, to make appropriate adjustments to the benefit-risk analysis process.

Uncertainties can come from multiple sources such as (but not limited to):

- Clinical relevance of key benefits and risks;
- Proper assignment of evaluation criteria to the key benefits and risks;
- Proper assignment of weights/functions to the benefits and risks;
- Proper assignment of aggregate functions to compare benefits and risks amongst themselves;
- Defined data relevance to the benefit-risk analysis;
- Data quality;
- Adequacy of the model used to perform the benefit-risk evaluation.

Several methods can be used to estimate these uncertainties:

- Statistical models and/or probabilistic models for weights/functions/parameters;
- Scenarios simulations;
- Experts group discussions and qualitative/meta analysis.

Funded by Horizon Europe Framework Programme of the European Union

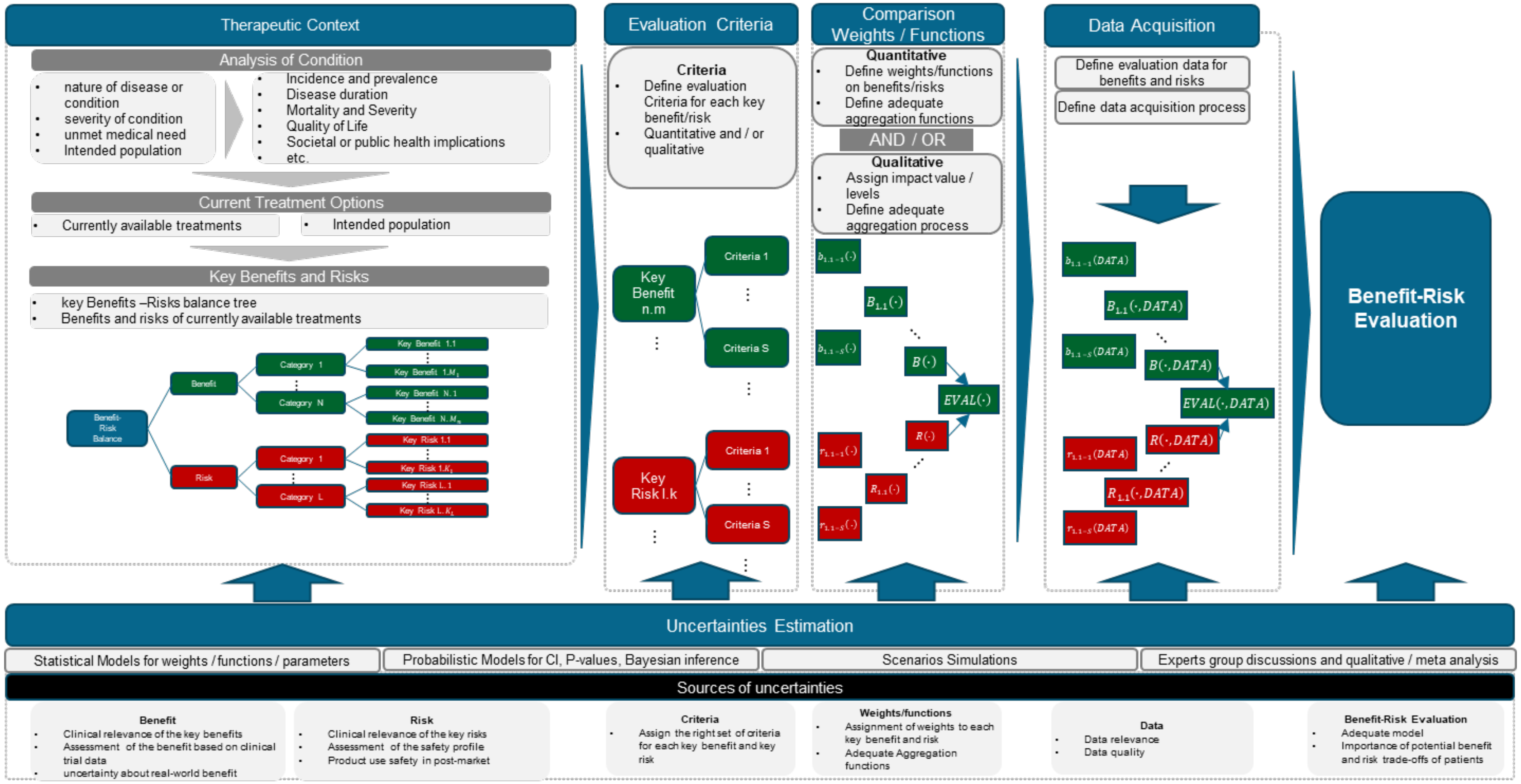

Therapeutic Context
Analysis of Condition
nature of disease or condition
severity of condition
unmet medical need
Intended population
Incidence and prevalence
Disease duration
Mortality and Severity
Quality of Life
Societal or public health implications
etc.
Current Treatment Options
Currently available treatments
Intended population
Key Benefits and Risks
key Benefits –Risks balance tree
Benefits and risks of currently available treatments
Benefit-Risk Balance
Benefit
Risk
Category 1
Category N
Category L
Key Benefit 1.1
Key Benefit 1.M1
Key Benefit N.1
Key Benefit N.MN
Key Risk 1.1
Key Risk 1.K1
Key Risk L.1
Key Risk L.KL
Evaluation Criteria
Criteria
Define evaluation Criteria for each key benefit/risk
Quantitative and / or qualitative
Key Benefit n.m
Key Risk l.k
Criteria 1
Criteria S
Comparison Weights / Functions
Quantitative
Define weights/functions on benefits/risks
Define adequate aggregation functions
AND / OR
Qualitative
Assign impact value / levels
Define adequate aggregation process
$b_{1.1-1}(\cdot)$
$b_{1.1-S}(\cdot)$
$B_{1.1}(\cdot)$
$B(\cdot)$
$EVAL(\cdot)$
$R(\cdot)$
$R_{1.1}(\cdot)$
$r_{1.1-1}(\cdot)$
$r_{1.1-S}(\cdot)$
Data Acquisition
Define evaluation data for benefits and risks
Define data acquisition process
$b_{1.1-1}(DATA)$
$B_{1.1}(\cdot, DATA)$
$b_{1.1-S}(DATA)$
$B(\cdot, DATA)$
$EVAL(\cdot, DATA)$
$R(\cdot, DATA)$
$r_{1.1-1}(DATA)$
$R_{1.1}(\cdot, DATA)$
$r_{1.1-S}(DATA)$
Benefit-Risk Evaluation
Uncertainties Estimation
Statistical Models for weights / functions / parameters
Probabilistic Models for CI, P-values, Bayesian inference
Scenarios Simulations
Experts group discussions and qualitative / meta analysis
Sources of uncertainties
Benefit
Clinical relevance of the key benefits
Assessment of the benefit based on clinical trial data
uncertainty about real-world benefit
Risk
Clinical relevance of the key risks
Assessment of the safety profile
Product use safety in post-market
Criteria
Assign the right set of criteria for each key benefit and key risk
Weights/functions
Assignment of weights to each key benefit and risk
Adequate Aggregation functions
Data
Data relevance
Data quality
Benefit-Risk Evaluation
Adequate model
Importance of potential benefit and risk trade-offs of patients

Figure 8 Benefit-Risk Scheme General View, from analysis performed on documents [11] and [10]

Funded by Horizon Europe Framework Programme of the European Union

5 Risk management tool

A Risk Management Tool with the purpose of enabling agile processes of risk management in healthcare has been designed and implemented. This section describes the first release of the tool.

Software Stack

The software stack of the first release of the Risk Management Tool is composed of a backend and a frontend, as illustrated by Figure 9.

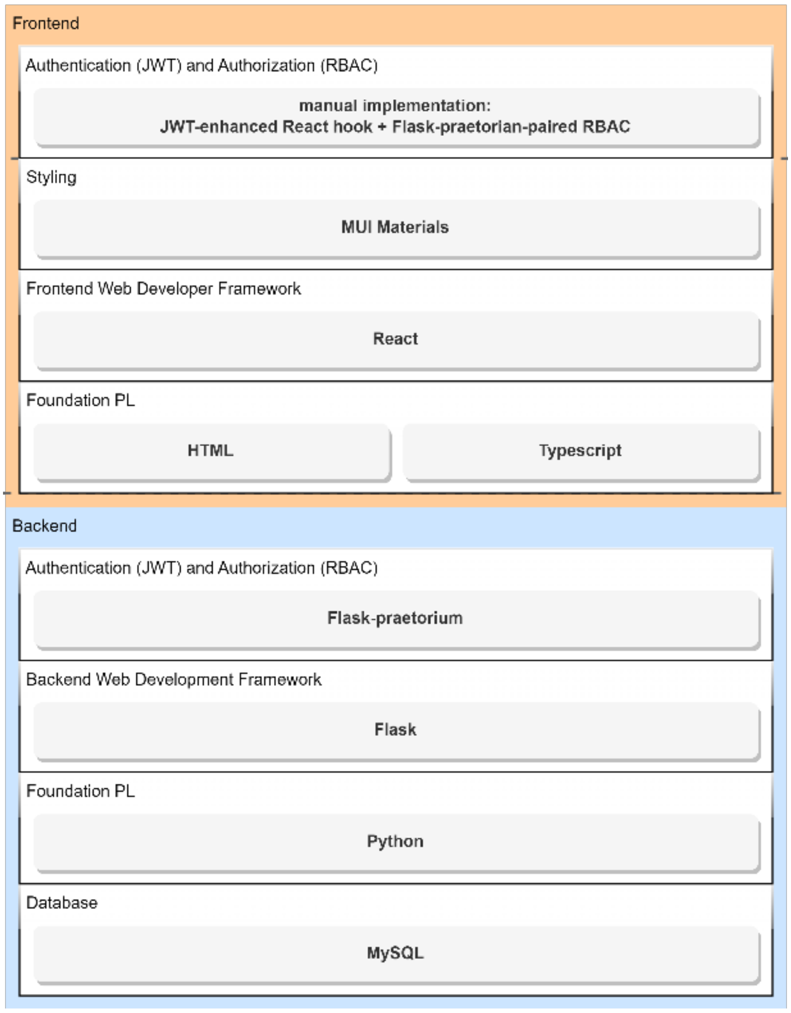

Frontend
Authentication (JWT) and Authorization (RBAC)
manual implementation:
JWT-enhanced React hook + Flask-praetorian-paired RBAC
Styling
MUI Materials
Frontend Web Developer Framework
React
Foundation PL
HTML
Typescript
Backend
Authentication (JWT) and Authorization (RBAC)
Flask-praetorium
Backend Web Development Framework
Flask
Foundation PL
Python
Database
MySQL

Figure 9 Risk Management Tool – software stack

The domain data is stored in a MySQL database server, which, depending on aspects of governance, security or incident management may be deployed together with the rest of the backend, or in a separate instance, managed independently.

The backend is powered by the Flask Python framework for web-development. This framework offers a variety of other libraries, the most relevant of which is `flask-praetorium`, which is used for JSON Web Token-based authentication and Role-Based Access Control and authorization.

The frontend is powered by the React renderer and the styling is achieved using MUI Materials. Authentication is achieved through a custom React hook that handles JSON Web Token requests when needed (e.g., refresh access token if it expires; or log user out if refresh token expires).

Funded by Horizon Europe Framework Programme of the European Union

Data Model

The data model of the Risk Management Tool is shown in Figure 10.

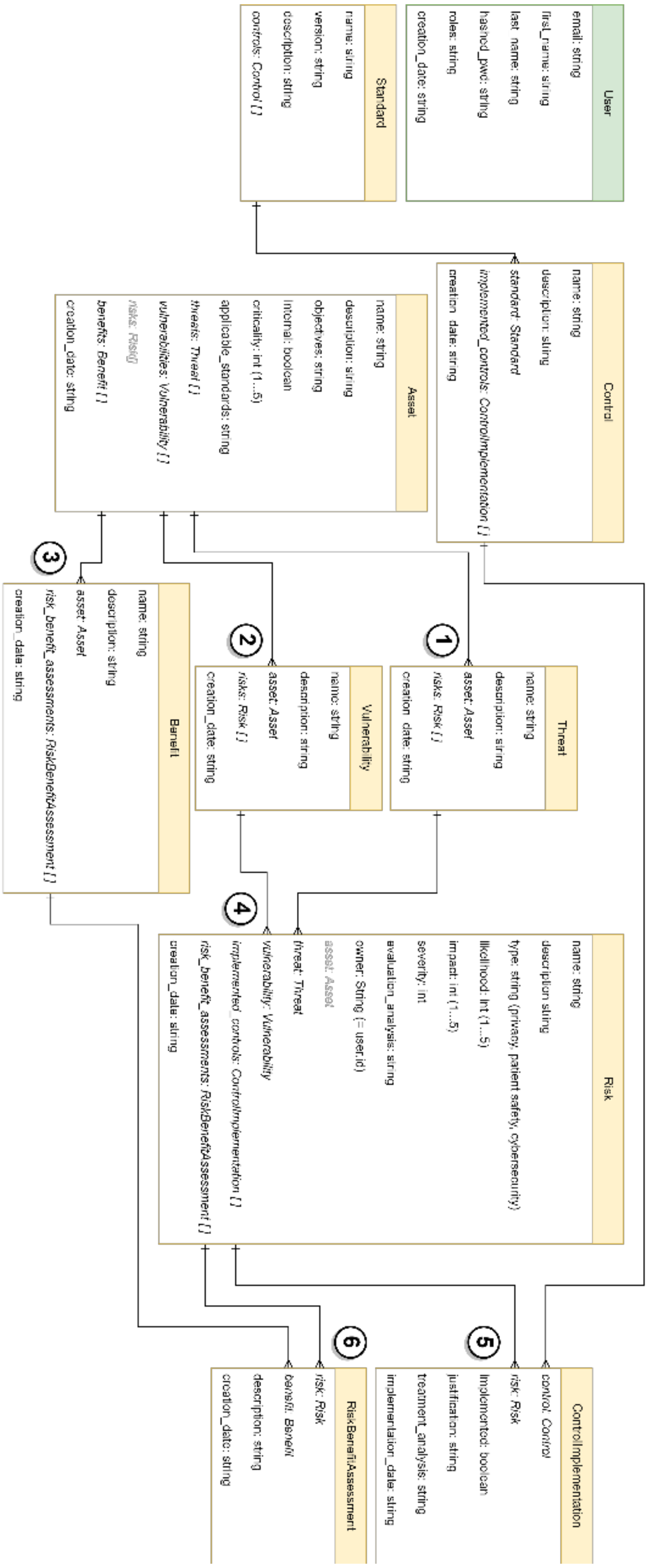


Figure 10 Risk Management Tool – data model

Funded by Horizon Europe
Framework Programme of the European Union

This data model is characterized by a unidirectional flow of relationships that avoids the common pitfalls of data model design (e.g., looping relationships), and clearly represents the relevant stages of the risk management process, starting with the documentation of standards and respective controls, as well as the assets. The process stages are numbered below, following the numbering of the data structure in Figure 10:

1. Threat assessment – process conducted for a given asset, resulting in a set of documented identified threats.
2. Vulnerability assessment – process conducted for a given asset, resulting in a set of documented identified vulnerabilities.
3. Benefit assessment – process conducted for a given asset, resulting in a set of documented identified benefits.
4. Risk assessment – process conducted for a given asset, dependent on the threat and vulnerability assessment processes, resulting in a set of documented identified risks.
5. Risk mitigation/treatment – process conducted for a given risk, aims to associate a control with a risk and to document the results of applying said control.
6. Risk-Benefit assessment – process conducted for a given asset, aims to associate a benefit with a risk and to document how said benefit would be impacted if the risk materialized.

The risk evaluation process is also implemented as a field in the risk object – `evaluation_analysis` – that can be filled and updated when appropriate.

The current iteration of the Risk Management Tool allows all of these processes to be performed on a basic level. In the frontend, the current representation is data-driven, meaning the focus is to represent all CRUD (Create, Read, Update, Delete) operations rather than make the presentation process-driven, as would be ideal for the end-user.

Authorization

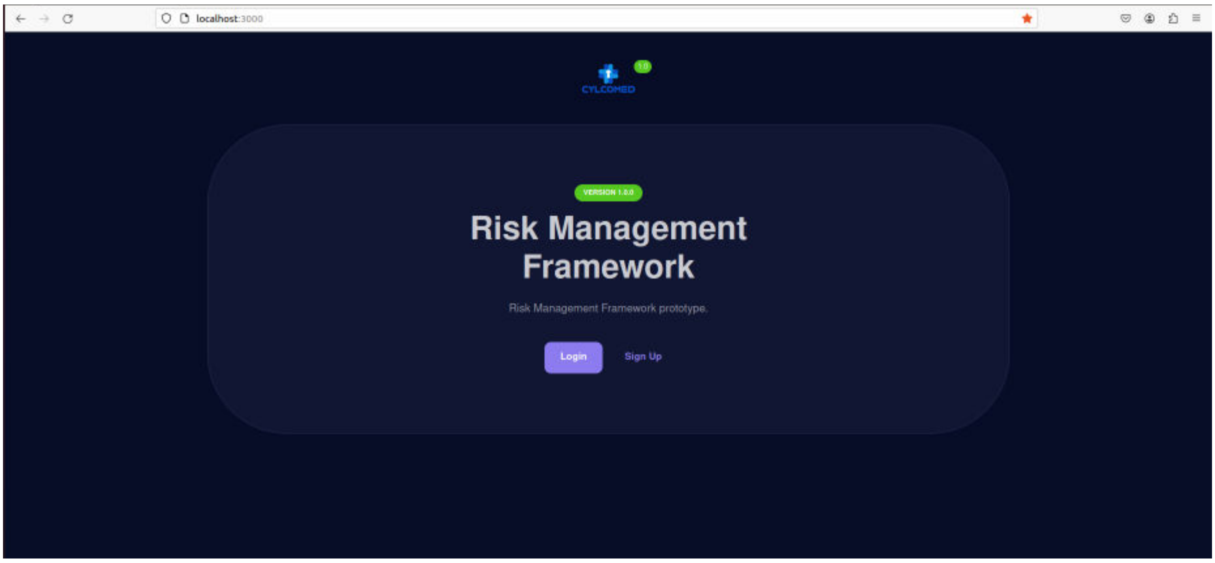
Authorization is based on Role-based Access Control (RBAC). Each user has an associated role:

- User Manager – this is the role that grants permissions to an account to manage the user-base, including the attribution of roles, or the deletion of accounts.
- Risk Manager – this is the role that grants permissions to an account to read, create, update and delete risk management data.
- Stakeholder – this is the role that grants permissions to an account to read risk management data.
- Pending – this is the default role of newly created accounts, and it means the user should wait for a User Manager to attribute the correct roles to the account.

Frontend

Upon opening the application, the user sees the screen presented in Figure 11.

Funded by Horizon Europe Framework Programme of the European Union

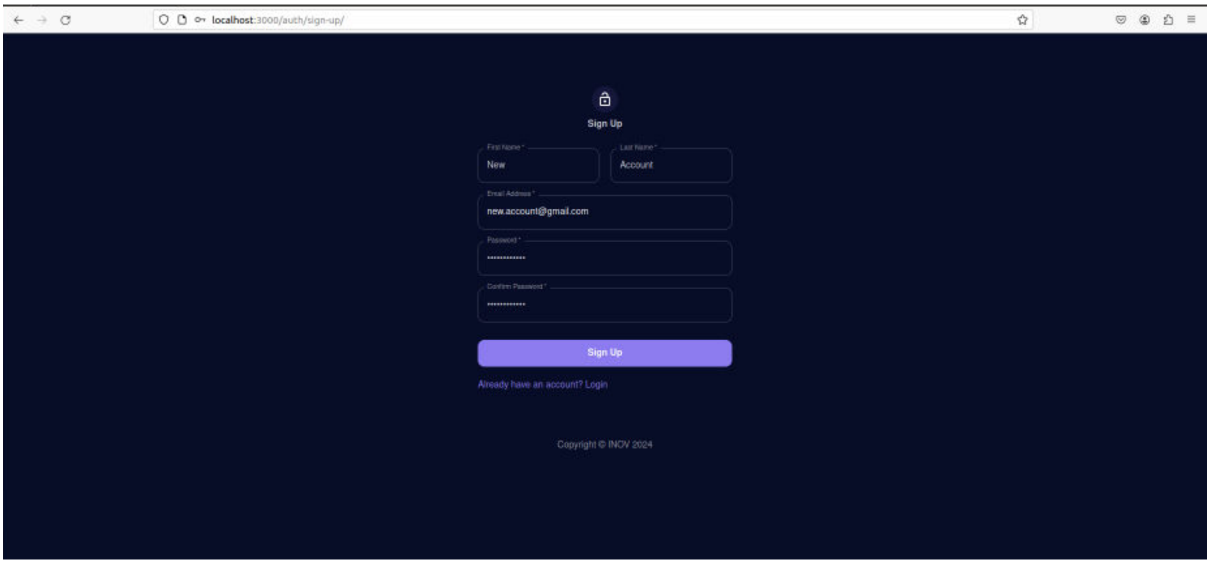


Risk Management Framework

Risk Management Framework prototype.

Figure 11 Risk Management Tool – homepage

From here the user can create an account by specifying his first and last name, his email and his preferred password twice, as seen in Figure 12.



Sign Up

First Name *: New

Last Name *: Account

Email Address *: new.account@gmail.com

Password *: ••••••••••••

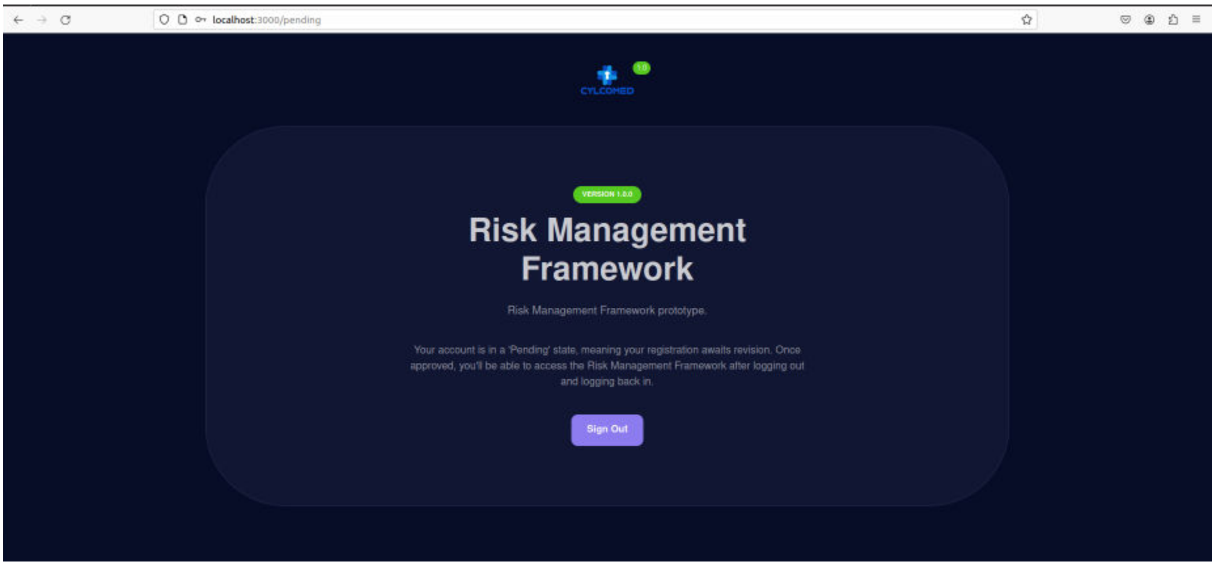
Confirm Password *: ••••••••••••

Copyright © INOV 2024

Figure 12 Risk Management Tool – sign up page – creating an account with first name “New”, last name “Account”, email “new.account@gmail.com” and a secret password.

If the new user logs in, he is greeted with the view of a Pending account, as seen in Figure 13.

Funded by Horizon Europe Framework Programme of the European Union



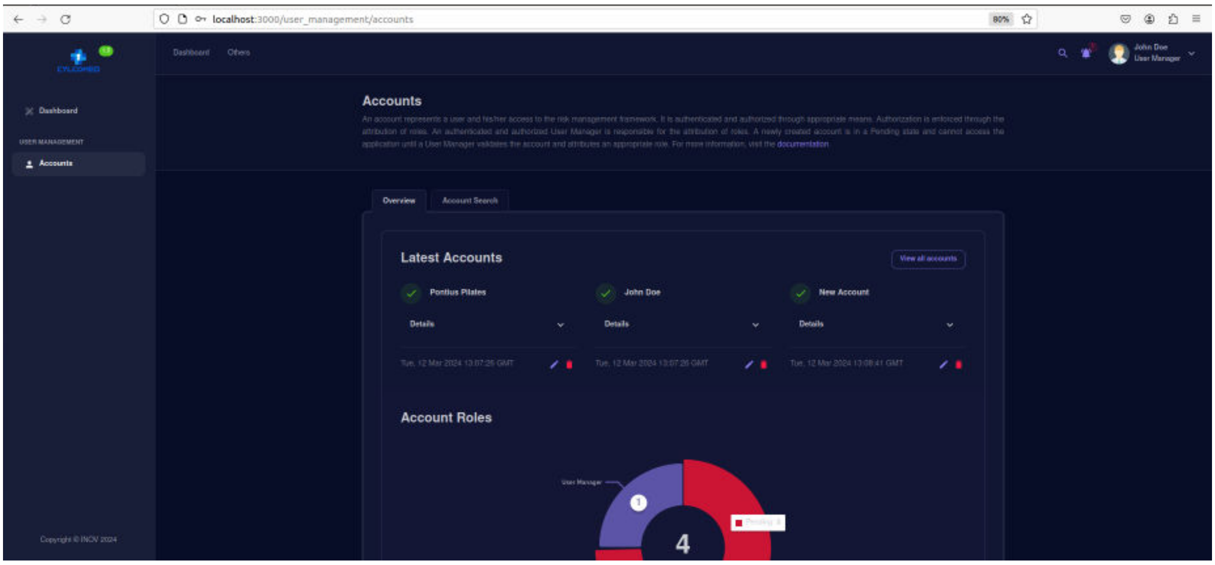
Risk Management Framework

Risk Management Framework prototype.

Your account is in a 'Pending' state, meaning your registration awaits revision. Once approved, you'll be able to access the Risk Management Framework after logging out and logging back in.

Figure 13 Risk Management Tool – view from the perspective of a "Pending" account

A user with an account with the User Manager role should attribute the relevant role to the newly created account. The view of the User Manager is as seen in Figure 14, the attribution of the role is seen in Figure 15.



Accounts

An account represents a user and his/her access to the risk management framework. It is authenticated and authorized through appropriate means. Authorization is enforced through the attribution of roles. An authenticated and authorized User Manager is responsible for the attribution of roles. A newly created account is in a Pending state and cannot access the application until a User Manager validates the account and attributes an appropriate role. For more information, visit the documentation.

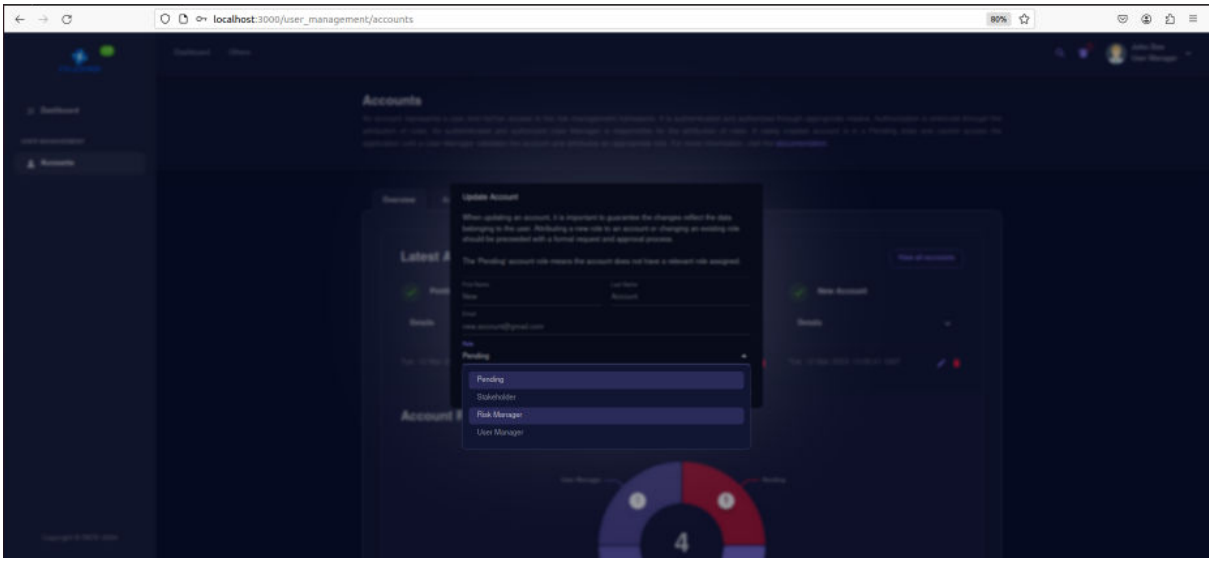
Latest Accounts

Pontius Pilates	John Doe	New Account
Details	Details	Details
Tue, 12 Mar 2024 13:07:26 GMT	Tue, 12 Mar 2024 13:07:26 GMT	Tue, 12 Mar 2024 13:08:41 GMT

Account Roles

Figure 14 Risk Management Tool – view from the perspective of an account with the User Manager role

Funded by Horizon Europe
Framework Programme of the European Union



Update Account

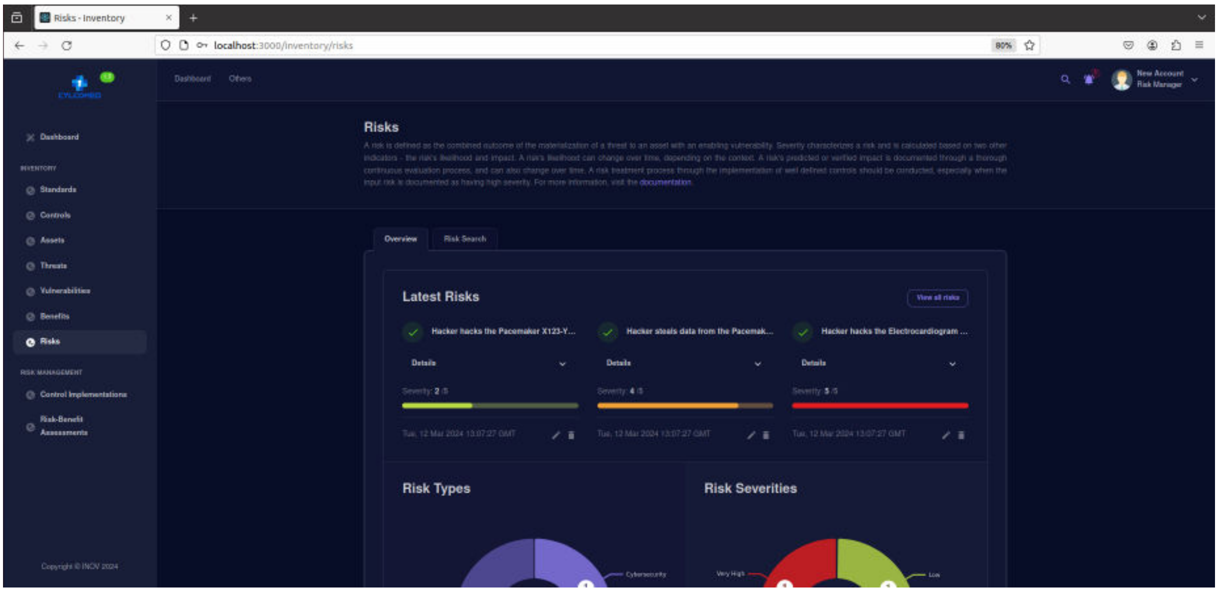
When updating an account, it is important to guarantee the changes reflect the data belonging to the user. Attributing a new role to an account or changing an existing role should be preceeded with a formal request and approval process.

The 'Pending' account role means the account does not have a relevant role assigned.

First Name: New
Last Name: Account
Email: new.account@gmail.com
Role: Pending

Figure 15 Risk Management Tool – User Manager attributes the Risk Manager role to the account with the name "New Account"

The User Manager attributes the Risk Manager role to the newly created account, so upon logging back in, the user who previously only had access to the view of a Pending account, now has access to the view of a Risk Manager. If the user accesses the page pertaining to the risks, the view is as seen in Figure 16.



Risks

A risk is defined as the combined outcome of the materialization of a threat to an asset with an enabling vulnerability. Severity characterizes a risk and is calculated based on two other indicators - the risk's likelihood and impact. A risk's likelihood can change over time, depending on the context. A risk's predicted or verified impact is documented through a thorough continuous evaluation process, and can also change over time. A risk treatment process through the implementation of well defined controls should be conducted, especially when the input risk is documented as having high severity. For more information, visit the documentation.

Latest Risks

Hacker hacks the Pacemaker X123-Y...
Severity: 2 /5
Tue, 12 Mar 2024 13:07:27 GMT

Hacker steals data from the Pacemak...
Severity: 4 /5
Tue, 12 Mar 2024 13:07:27 GMT

Hacker hacks the Electrocardiogram ...
Severity: 5 /5
Tue, 12 Mar 2024 13:07:27 GMT

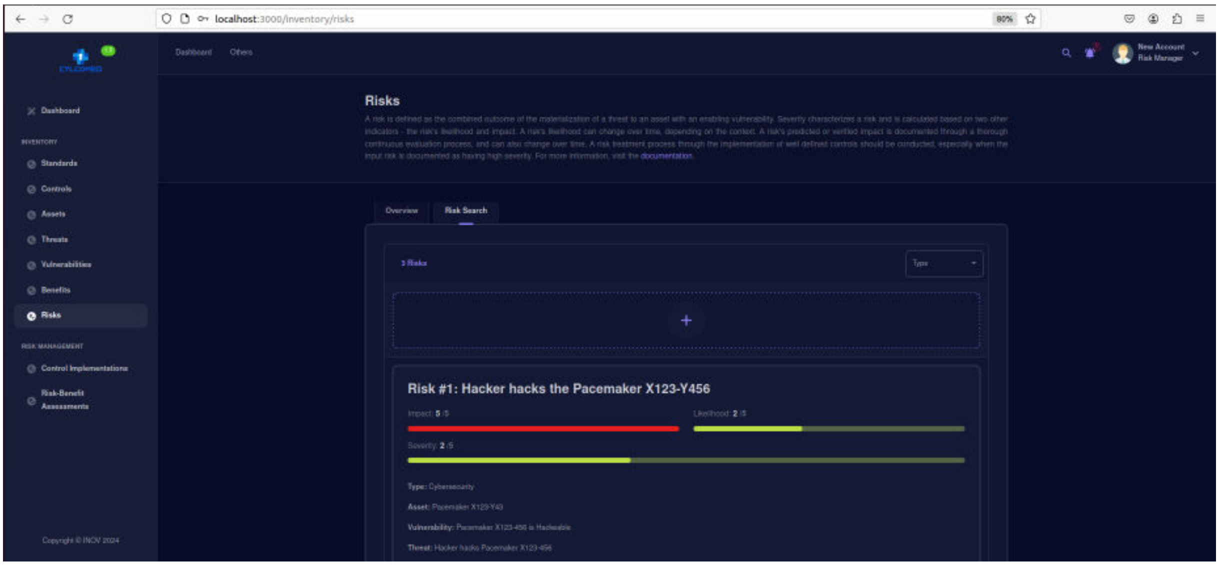
Risk Types

Risk Severities

Figure 16 Risk Management Tool – view from the perspective of an account with the Risk Manager role – "Overview" tab from the `inventory/risks` *page*

Alternatively, the Risk Manager also has access to another tab with a more holistic view of all information, as seen in Figure 17.

Funded by Horizon Europe
Framework Programme of the European Union



Risks

A risk is defined as the combined outcome of the materialization of a threat to an asset with an enabling vulnerability. Severity characterizes a risk and is calculated based on two other indicators - the risk's likelihood and impact. A risk's likelihood can change over time, depending on the context. A risk's predicted or verified impact is documented through a thorough continuous evaluation process, and can also change over time. A risk treatment process through the implementation of well defined controls should be conducted, especially when the input risk is documented as having high severity. For more information, visit the documentation.

Risk #1: Hacker hacks the Pacemaker X123-Y456

Impact: 5 /5

Likelihood: 2 /5

Severity: 2 /5

Type: Cybersecurity

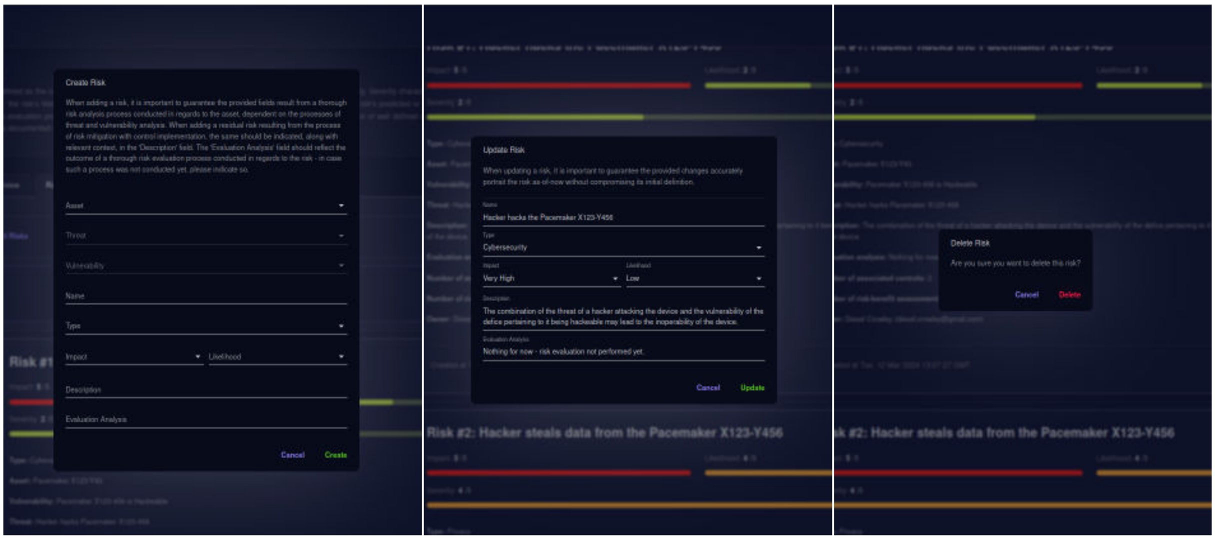
Asset: Pacemaker X123-Y43

Vulnerability: Pacemaker X123-456 is Hackeable

Threat: Hacker hacks Pacemaker X123-456

Figure 17 Risk Management Tool – view from the perspective of an account with the Risk Manager role – "Risk Search" tab from the `inventory/risks` *page*

The Risk Manager has access to creation, update and deletion forms, as seen in Figure 18.



Create Risk

When adding a risk, it is important to guarantee the provided fields result from a thorough risk analysis process conducted in regards to the asset, dependent on the processes of threat and vulnerability analysis. When adding a residual risk resulting from the process of risk mitigation with control implementation, the same should be indicated, along with relevant context, in the 'Description' field. The 'Evaluation Analysis' field should reflect the outcome of a thorough risk evaluation process conducted in regards to the risk - in case such a process was not conducted yet, please indicate so.

Asset

Threat

Vulnerability

Name

Type

Impact

Likelihood

Description

Evaluation Analysis

Cancel Create

Update Risk

When updating a risk, it is important to guarantee the provided changes accurately portrait the risk as-of-now without compromising its initial definition.

Name: Hacker hacks the Pacemaker X123-Y456

Type: Cybersecurity

Impact: Very High

Likelihood: Low

Description: The combination of the threat of a hacker attacking the device and the vulnerability of the defice pertaining to it being hackeable may lead to the inoperability of the device.

Evaluation Analysis: Nothing for now - risk evaluation not performed yet.

Cancel Update

Delete Risk

Are you sure you want to delete this risk?

Cancel Delete

Figure 18 Risk Management Tool – on the left, form to create a Risk register; on the center, form to update an existing Risk register; on the right, form to delete a Risk register

It is important to note that in order to update or delete a risk, the account must be the owner of the risk – the "New Account" that has been created earlier was not the owner of the currently listed rRisks, and that is why the update and delete icons are greyed-out in Figure 15. In order to see the update and delete forms shown in Figure 18, the page is being viewed from the perspective of the risk owner.

As for accounts with the Stakeholder role, these have access to a similar interface to that of the Risk Manager, but without access to the create, update and delete buttons, allowing the user to only read the data.

The figures show the page pertaining to risks (i.e. `inventory/risks`), but the pages for the remaining elements of the data models follow a similar structure.

It is also important to note that the styling of the frontend shown in the figures, with the dark purple hue, may not represent the final styling of the tool.

Funded by Horizon Europe Framework Programme of the European Union

Conclusions

This deliverable documents the ongoing summary of the risk-benefit analysis techniques and the current status of the risk management tool for connected medical devices.

In this report, the risk analysis of connected medical devices was tackled taking into account the ISO 14971:2019 standard and the accompanying ISO 24971 document, as these documents serve as guidance for manufacturers in keeping their product safe for patients and for the compliance of regulations. Moreover, benefit-risk analysis schemes were thoroughly researched and analysed, and a generalized benefit-risk analysis scheme was developed to deliver a common understanding of all the analysed benefit-risk analysis schemes. This benefit-risk analysis methodology will be further explored in specific MDs within the CYLCOMED project, and improved considering the feedback from relevant stakeholders (e.g., IT professionals, cybersecurity experts from hospitals).

A risk management tool is in development. The first release supports a data-driven interface with the purpose of testing and validating the data model. Subsequent releases will aim towards the implementation of process-driven views. As the project proceeds, the tool will evolve taking into account the user experience and new requirements that might emerge.

References

[1] Bijan Elahi, “Quantification of Beneefits for Medical Devices,” vol. 58, no. 1, 2023.

[2] Rodrigues, Joel & Segundo, Dante & Arantes Junqueira, Heres & Sabino, Murilo & Prince, Rafael & Al-Muhtadi, Jalal & Albuquerque, Victor, “Enabling technologies forthe Internet of Health Things,” *IEEE Access,* 2018.

[3] Samuel Wairimu, Lothar Fritsch, “Modelling privacy harms of compormised personal medical data - beyond data breach,” in *Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22)*, New York, 2022.

[4] British Standards Institution (BSI), “Risk management for medical devices and the new BS EN ISO 14971,” British Standards Institution (BSI).

[5] Stephen G. Odaibo, “Risk Management of AI/ML Software as a Medical Device (SaMD): On ISO 14971 and Related Standards and Guidances,” *ArXiv,* no. abs/2109.07905, 2021.

[6] International Organization for Standardization, “Recognition of En ISO 14971 as a harmonized standard in support of the European Medical Device Regulations,” [Online]. Available: https://committee.iso.org/sites/tc210/home/news/content-left-area/news-and-updates/recognition-of-en-iso-14971-as-a.html. [Accessed 11 2023].

[7] Lowry, Svetlana & Quinn, Matthew & Ramaiah, Mala & Schumacher, Robert & Patterson, Emily & North, Robert & Zhang, Jiajie & Gibbons, Michael & Abbott, Patricia., “Technical Evaluation, Testing, and Validation of the Usability of Electronic Health Records,” 2023.

[8] “ISO 14971:2019 Medical devices - Application of risk management to medical devices”.

[9] ISO, “ISO/TR 24971:2020 Medical devices - Guidance on the application of ISO 14971”.

[10] PROTECT Consortium, “Review of methodologies for benefit and risk assessment of medication,” 2013.

[11] COuncil for International Organizations of Mecical Sciendes Working Group, “Benefit-Risk Balance for Medicinal Products,” Switzerland, 2023.

[12] CJ Mann, “Observational research methods. Research design II: cohort, cross secitonal, and case-control studies,” *Emergency medicine journal,* no. 20, pp. 4-60, 2003.

[13] Nina Kauffmann, Felix Fahrenkrog, Ludwig Drees and Florian Raisch, “Positive risk balance: a comprehensive fraework to ensure vehicle safety,” *Ethics and Information technology,* vol. 24, no. 15, 2022.

[14] U.S. Department of Health and Human Services Food and Drug Administration, “Benefit-Risk Assessment for New Drug and Biological Products - Guidance for Industry,” 2023.

Funded by Horizon Europe
Framework Programme of the European Union