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

D4.3 RISK BENEFIT SCHEME AND RISK MANAGEMENT TOOL

Revision: v.1.0

Work package	WP 4
Task	Task 4.2
Due date	31/03/2025
Submission date	10/04/2025
Deliverable lead	INOV
Version	0.1
Authors	João Rodrigues (INOV), Gonçalo Cadete (INOV)
Reviewers	Pietro Di Maggio (MCI), Simone Favrin (MCI)

Abstract	This document reports the risk management tool that has been developed for the project, the cybersecurity risk management framework and the benefit-risk analysis methodology for evaluating the benefits and the risks of Connected Medical Devices.

Keywords	Connected Medical Devices, Risk Management Tool, Risk Management Framework, Safety, Threat, Risk, Vulnerability, Benefit-Risk Analysis

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V0.1	01/02/2025	Table of Content	João Rodrigues, Gonçalo Cadete
V0.2	18/03/2025	Version ready for internal review	João Rodrigues, Gonçalo Cadete
V0.3	28/03/2025	Internal Review	Andrea Scaburri, Simone Favrin
V0.4	04/04/2025	Version ready for second internal review	João Rodrigues, Gonçalo Cadete
V1.0	09/04/2025	Final Version	João Rodrigues, Gonçalo Cadete

Disclaimer

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

Funded by Horizon Europe Framework Programme of the European Union

ETHICS: Deliverables related to ethics issues.
SECURITY: Deliverables related to security issues
OTHER: Software, technical diagram, algorithms, models, etc.

Funded by Horizon Europe Framework Programme of the European Union

Executive summary

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. On the other hand, many medical devices lack built-in security features, others have outdated operating systems, hardcoded credentials, weak authentication mechanisms and limited resources (memory and computing capabilities), making them vulnerable to a wide range of attacks.

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;
- 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 was 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, NIST CSF 2, NIST RMF;
- 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.

Funded by Horizon Europe Framework Programme of the European Union

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

Funded by Horizon Europe Framework Programme of the European Union

Table of contents

Funded by Horizon Europe Framework Programme of the European Union

Funded by Horizon Europe Framework Programme of the European Union

List of figures

Funded by Horizon Europe Framework Programme of the European Union

Funded by Horizon Europe Framework Programme of the European Union

List of tables

Funded by Horizon Europe Framework Programme of the European Union

Abbreviations

5G	Fifth Generation technology standard for cellular networks
5G AKA	5G Authorization and Key Agreement
AI	Artificial Intelligence
APP	Applications
AR	Augmented Reality
AT&T	American Telephone and Telegraph
BSI	Bundesamt für Sicherheit in der Informationstechnik, German Federal Office for Information Security
CMD	Connected Medical Device
CON	Concepts
CSF	Cybersecurity Framework
DAO	Decentralized Autonomous Organization
DER	Detection and Reaction
DDOS	Distributed Denial of Service
DOS	Denial of Service
DPOS	Distributed Proof Of Stake
eMBB	Enhanced Mobile Broadband
EVM	Ethereum Virtual Machine
FMEDA	Failure Modes, Effects, Diagnosis Analysis methodology
GDPR	General Data Privacy Regulation
IDSA	International Data Spaces Association
IEC	International Electrotechnical Commission
IoMT	Internet of Medical Things
IoT	Internet of Things
ISMS	Information Security Management System
ISO	International Organization for Standardization
IVDR	In Vitro Diagnostics Regulation
IVDR	In Vitro Diagnostics
JTC	JointTechnical Committee
MDR	Medical Device
MDR	Medical Device Regulation
MEC	Multi-Access Edge Computing
mMTC	Massive Machine-Type Communication
MRI	Magnetic Resonance Imaging
NET	NEtworks and Communication
NIST	National Institute for Standards and Technology
OPS	Operations
ORP	ORganisation and Personnel
OWASP	Open Web Application Security Project
PACS	Picture Archiving and Communication System
PDCA	Plan, Do, Check, Act process cycle
POS	Proof Of Stake
POW	Proof of Work
RMF	Risk Management Framework
SaMD	Software as a Medical Device
SIEM	Security Information and Event Management
SYS	IT System

Funded by Horizon Europe Framework Programme of the European Union

TR	Technical Report
URLCC	Ultra-reliable and Low Latency Communications
VR	Virtual Reality

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]. On the other hand, as highlighted in [2], many medical devices lack built-in security features, others have outdated operating systems, hardcoded credentials, weak authentication mechanisms and limited resources (memory and computing capabilities), making them vulnerable to a wide range of attacks.

For instance, unpatched software and outdated firmware will maintain known software flaws and outdated security measures, which could be exploited. These include weak cryptographic protocols and buffer overflow vulnerabilities, among others.

Being able to access, inadvertently, medical devices in the hospital environment is also a major concern. The device could be stolen, or even tampered with, making patient data vulnerable, as well as the correct functioning of the device.

Other vulnerabilities are due to the high-connectivity nature of such devices. Network and communication vulnerabilities include open ports, weak or non-existing encryption mechanisms (e.g., due to limited resources, or outdated software), insecure network protocols (e.g., due to outdated software), and wireless based attacks (jamming attacks, eavesdropping, replay attacks and injection attacks.

These devices usually communicate with cloud services. If data storage is done with improper encryption, improper access control mechanisms, or improper data integrity mechanisms, several incidents, like data breaches and unauthorized changes to data (including ransomware), could occur.

Moreover, with the aforementioned vulnerabilities, if CMDs are not deployed appropriately within the hospital infrastructure (connection with the hospital's network and other devices), the aforementioned vulnerabilities could be exploited to make an even larger scale attack, like a DDoS to the hospital.

Moreover, the lack of cybersecurity awareness and training also contribute immensely to the existence of vulnerabilities, leading phishing and social engineering attacks to be successfully used to gain access to login credentials and sensitive information.

Also, misuse of privileges, also known as insider threats, can occur, as a result of social engineering, or personal motivation.

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);

Funded by Horizon Europe Framework Programme of the European Union

- 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;
- 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 was 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, NIST CSF 2, NIST RMF;
- 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.

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

1.1 Methodology

The work done to develop the Risk Management Tool, the benefit-risk scheme and the risk management framework was built on top of previously documented work on:

- survey existing benefit-risk schemes used within the healthcare sector, and the generalization of the benefit-risk scheme which was shared and validated by the consortium;
- initial design of the risk management tool, building from previous study on risk management frameworks;
- The generalization of the benefit-risk schemes carried out, which was shared and validated by the consortium for the first release.

The final Benefit-risk scheme resulted from:

- The analysis of risk factors usually used to evaluate medical devices;
- The analysis of risk factors usually used by healthcare providers;
- The analysis of risk factors usually used in cybersecurity;
- The multitude of therapeutic areas;
- The most generic framework for evaluating multiple criteria, in a qualitative manner;
- Validation from the consortium.

The Risk Management Framework focused on cybersecurity of connected medical devices, resulted from:

- Extensive analysis of cybersecurity risk management frameworks, such as the ISO 27001, 27002, NIST CSF 2, NIST RMF;

Funded by Horizon Europe Framework Programme of the European Union

- Documents regarding cloud, IoT, Blockchain, AI, 5G architecture, risk management framework and cybersecurity;
- Organization of cybersecurity core controls into 10 main categories, with shared responsibilities among the manufacturer, the healthcare provider and the patient.
- Validation by the consortium.

The final Risk Management Tool resulted from:

- Design and development, taking into account a process view, to align with the risk management framework;
- Validation by the consortium.

1.2 Structure of the document

This report is structured as follows:

- Section 2 starts with a brief introduction of risk management, giving emphasis on the risk criteria and benefits, which are crucial parts of the Benefit-risk scheme.
- In Section 3, the CYLCOMED Benefit-risk is described, including all the components to determine the impact of cybersecurity measures in the CMD risks and benefits.
- In section 4, the CYLCOMED risk management framework is described as a natural combination of the manufacturers' risk management process, the hospitals' risk management process, and the CYLCOMED benefit-risk scheme.
- Section 5 is dedicated to the description 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

2.1 Threats, Vulnerabilities and Risks

An organization is composed of assets, which can be any item, hardware, buildings, software, people, information, which adds value to the organization's strategies and objectives. They all work in combination to form useful processes for the business units of the organization, aiming at fulfilling the defined strategies and objectives.

Assets are subject to threats, anything that can cause an unwanted incident, leading to an adverse event to the organization. Examples of such threats include natural disasters like hurricanes, floods or wildfire, that can damage buildings and any assets within, as well as hacker activities. Threats are inherently uncertain as they are exterior factors that an organization cannot control.

Also, assets may have vulnerabilities, which are weaknesses that, combined with certain threats, can lead to harmful events to the organization. A vulnerability is something that is inherent to an organization, something that can be controlled.

A risk exists whenever your organization is exposed to a threat that can exploit some existing vulnerability. Examples of this are depicted in Figure 1.

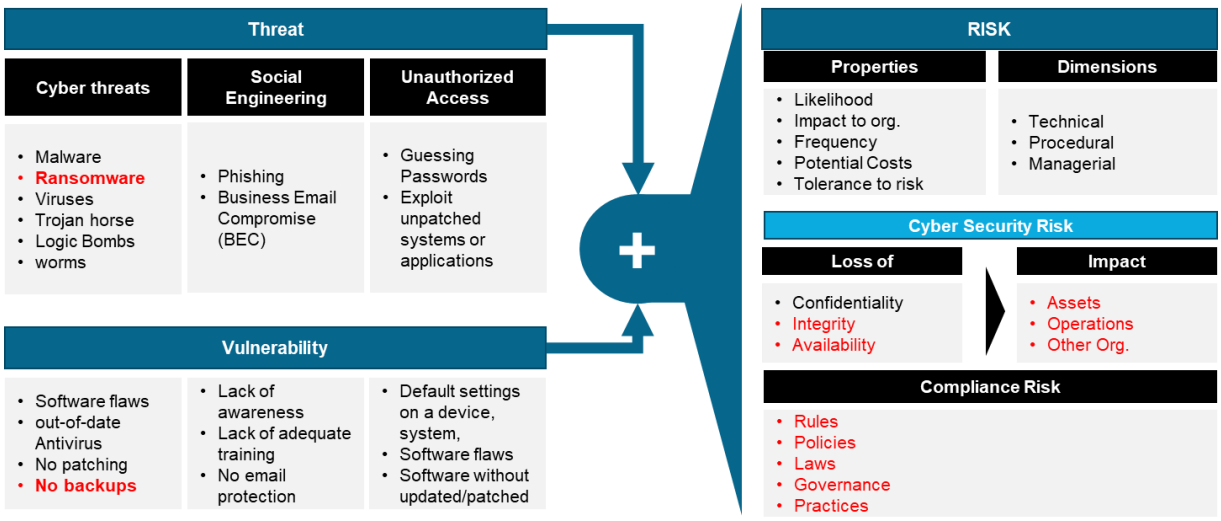

Figure 1 Relationship between threat, vulnerability and risk with some examples in the context of cybersecurity. An example of combination of a threat and vulnerabilities, and potential impact areas are marked in red

If an organization has no backup mechanisms in place (vulnerability) then, for example, a ransomware attack (a threat, which is uncertain when and how it will occur) will impact the assets of the organization, which will impact the operations and can potentially have negative consequences to other organizations. Depending on the organization's business nature, this event can potentially result in fines or any other penalties resulting from non-compliance with laws, regulations, policies or best practices.

Risks can be of technical, procedural or managerial nature, and they present the following properties:

- Likelihood;
- Impact;
- Frequency;
- Potential costs;
- The organization's tolerance to risk;

Funded by Horizon Europe Framework Programme of the European Union

- Likelihood;Impact to the organization;
- Potential costs;

2.2 Risk Management Process

Risk management is the process by which threat uncertainties and their effects on the organization's objectives are managed and controlled [3]. It involves the establishment of a governance structure, definition and application of policies, processes and procedures and coordination of all activities related to risk management.

According to ISO/IEC 31000 – Risk Management Guidance, risk management has the following 6 stages:

- **Establish the Context**, which is the stage where the organization's context is understood. The organization context includes their strategies, objectives, internal and external stakeholders, internal and external environment, business unit needs, roles and responsibilities, legal requirements, standards to follow, policies. In this stage it is also defined what is the scope of the risk management process (e.g., a business unit process, an IT system). It is in this phase that the risk criteria[1] / risk appetite is defined, in order to guide further the management process. It also defines the risk significance evaluation to support decision-making.

- **Risk Assessment**, which is comprised of 3 phases:
  - risk identification which refers to the identification of the organization's artifacts that are relevant to business objectives, the associated threats, any countermeasures that are already implemented and the existing vulnerabilities
  - risk analysis which refers to the evaluation of the relevant scenarios of risk (combination of risks and vulnerabilities), their likelihood of happening and their impact. The risk level is determined by the likelihood and the impact.
  - risk evaluation, which compares the estimated risks with the risk criteria.
- **Risk Treatment,** is the stage where the selection of the most appropriate risk treatment measure(s), processes, procedures and plans take place. There are four possible ways to deal with risk:
  - avoid the risk;
  - accept the risk;
  - mitigate the risk;
  - transfer the risk.

- **Communication and Consultation**, which serves two purposes. First, it aims to bring together knowledge of different areas of expertise to better inform and guide the risk management efforts (e.g., risk analysis and oversight, decision making). Second, it aims to inform all relevant parties about the risk management activities.

- **Risk Monitoring and review**, the stage that aims at evaluating the effectiveness of the implemented risk management process, review any changes in context (internal and external) that could imply changes to the implemented risk management controls or processes and guarantee that the defined roles are fulfilling their responsibilities.
- **Recording and Reporting**: stage that keeps records of every relevant information regarding the activities and results of the risk management process (e.g., changes to

[1] *According to NIST, risk criteria is defined as the terms of reference against which the significance of a risk is evaluated, such as organizational objectives, internal/external context, and mandatory requirements (e.g., standards, laws, policies)*

Funded by Horizon Europe Framework Programme of the European Union

the process, decision making, communication with relevant entities/people), provides relevant risk information for decision making and for relevant stakeholders.

Having the proper leadership is crucial to the correct functioning of the Risk Management Process. Executive members should be included in the decision-making process.

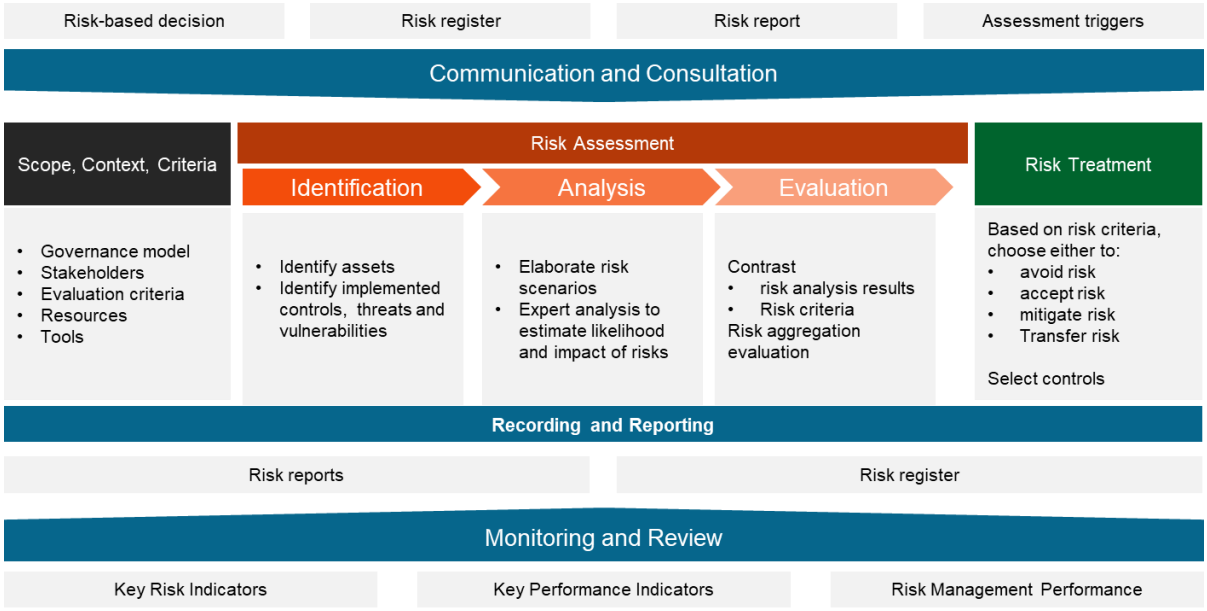

Figure 2 Risk Management Framework phases according to ISO 31000

2.3 Risk Criteria

The **risk acceptability criteria** are a crucial component to integrate into the cybersecurity risk management framework, as it incorporates factors to be considered when evaluating risks and benefits, the likelihood (frequency or probability scale of some risk to materialize), the impact of the risk should it be materialized.

One example of a qualitative risk impact level is the following Severity Categories [4]:

- **Insignificant**: No treatment required.
- **Minor**: Requires first aid.
- **Moderate**: Needs medical treatment.
- **Major**: Hospitalization or long-term disability.
- **Catastrophic**: Fatality or permanent impairment.

The likelihood scale would look like this [4], [5] [6]:

- **Rare:** May happen only in exceptional circumstances (<5% probability).
- **Unlikely:** Could happen but not expected (5-30%).
- **Possible:** Might occur occasionally (30-70%).
- **Likely:** Expected in most situations (70-95%).
- **Almost Certain:** Will undoubtedly occur (>95%).

The Risk Matrix is a tool that helps determine the risk level, by combining the risk severity and the likelihood. It is usually colour coded in the following way [5] (see Figure 3 for an example):

- **Very High Risk (Red):** Immediate action required.

Funded by Horizon Europe Framework Programme of the European Union

- **High Risk (Orange):** Mitigation necessary within a defined timeframe.
- **Moderate Risk (Yellow):** Needs monitoring and controls.
- **Low Risk (Green):** Minimal intervention required.

	Consequence Score				
Likelihood	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain					
Likely					
Possible					
Unlikely					
Rare					

Figure 3 Example of a Risk Matrix for the typical severity categories and likelihood scores. Colouring code varies according to context

The risk matrix enables the definition of the risk appetite and risk tolerances. The risk tolerance is the amount of risk an organization is willing to accept to achieve its objectives.

Risk Factors in healthcare always include Clinical and patient safety risks, but other factors must also be considered.

Clinical & Patient Safety Risks are risks that affect patient health, treatment outcomes or safety [5], [6]. Examples include:

- Medication errors (e.g., incorrect drug dosages, labelling issues);
- Delayed emergency response times;
- Delayed treatment or misdiagnosis due to IT failures or staff shortages;
- hospital-acquired infections.

Workforce & Staffing Risks are risks related to staff shortages, burnout, retention and or training deficiencies [5], [6]. It includes:

- High turnover rates leading to operational inefficiencies;
- Burnout due to excessive workloads;
- Shortage of specialists in critical departments.

Financial Risks are risks that affect the financial sustainability of healthcare services**.** It includes:

- Budget deficits affecting service delivery.
- Unexpected cost increases (e.g., inflation-driven expenses).
- Unfunded capital projects leading to operational constraints.
- Unrecoverable debts from commissioners or external partners.
- Cost overruns in infrastructure projects.

Operational & IT Risks are risks related to the disruption of normal hospital or IT operations [5]**.** Examples include:

- System downtime affecting patient record access;
- Failure of cybersecurity controls leading to data breaches;

Funded by Horizon Europe Framework Programme of the European Union

- Poor integration between healthcare IT systems.

Information Security and Cyber Risks are risks related to data breaches, cyberattacks, and IT system failures [6]. They include:

- Unauthorized access to patient records due to weak cybersecurity protocols;
- Failure of IT infrastructure**,** impacting hospital operations;
- Ransomware attacks targeting hospital systems**.**

Compliance & Regulatory Risks are risks related to failing to meet legal, ethical, or NHS regulatory requirements [5], [6]. They include:

- Failure to meet national patient safety targets;
- Non-compliance with Care Quality Commission (CQC) standards;
- Failure to meet national patient safety requirements;
- Data protection violations (e.g., breaches of GDPR rules).

Reputational Risks are risks that could damage public trust and reputation [6]**.** They include:

- Negative media coverage due to patient harm incidents;
- Public dissatisfaction with waiting times and hospital care**;**
- Social media controversies affecting NHS leadership credibility**;**

Environmental and Business Continuity Risks are risks that could disrupt the hospital's operations due to external events [6]. They include:

- Pandemic outbreaks affecting service delivery**;**
- Flooding, fires, or natural disasters impacting hospital infrastructure.

Particularizing to medical devices, risk considerations can include [7]:

Table 1 Risk considerations for medical devices, according to [7]

Risk Considerations	Description
Severity of Harm	Categorized into three levels: serious injuries/deaths, non-serious adverse events, and events without reported harm.
Medical Device-Related Deaths or Serious Injuries	Includes events attributed to device use that cause or contribute to death, life-threatening illness, or permanent impairment.
Medical Device-Related Non-Serious Adverse Events	Covers events leading to minor, temporary, or medically reversible injuries that do not classify as serious injuries.
Medical Device-Related Events Without Reported Harm	Encompasses nonconformities or malfunctions with no related harm, including regulatory noncompliance detected at manufacturing.
Likelihood of Risk	Assesses the probability of a device problem occurring, patient exposure to harm, and overall risk to the patient population.
Distribution of Nonconforming Devices	Determines if and how many nonconforming devices have been distributed in the market.
Duration of Exposure to Population	Measures the time between patient exposure to the risk and when the risk is successfully mitigated.
False-Positive or False-Negative Results	Considers the consequences of incorrect diagnostic results, such as unnecessary treatment (false-positive) or missed treatment (false-negative).

Funded by Horizon Europe Framework Programme of the European Union

Risk Considerations	Description
Patient Tolerance of Risk	Examines patient willingness to accept risks, including those associated with nonconforming devices or manufacturer non-compliance.
Risk Factors for Healthcare Professionals or Caregivers	Evaluates risks that may impact healthcare professionals or caregivers, including usability and safety concerns.

2.4 Benefits

Also important is the definition of the benefits of the CMD. Considerations that should be taken into account can include [7]:

Table 2 Benefits considerations according to [7]

Benefit Factor	Description
Type of Benefit(s)	Includes impact on patient health and clinical management, quality of life, survival, daily activities, and symptom relief. Clinicians may discover additional benefits over time.
Magnitude of Benefit(s)	Degree to which patients experience the treatment benefit or the effectiveness of the device. Assessed against standards of care and expected performance, which may change over time.
Likelihood of Patients Experiencing Benefit	Likelihood that the device will effectively treat or diagnose a condition. Can vary among subpopulations, where certain groups may experience greater benefits.
Duration of Effects	How long the benefit lasts. Curative treatments typically provide higher benefits due to longer-lasting effects. Real-world evidence may show effects longer than initial clinical data.
Patient Perspective on Benefit	Value placed by patients on the device, especially in severe or chronic conditions. Patients with life-threatening conditions may value short-term extensions more than those with minor conditions.
Benefit Factors for Healthcare Professionals or Caregivers	improvements in patient care, clinical practice, procedural time reduction, and utility for healthcare providers with different skill levels.
Medical Necessity	Assessment of whether the device addresses an unmet need or if an alternative therapy exists. Availability of substitutes should be considered.

Funded by Horizon Europe Framework Programme of the European Union

3 Benefit-risk scheme

When designing and manufacturing a CMD, according to ISO 14971, the manufacturer needs to determine the benefits of the device and predict the hazardous situations arising from foreseeable use and foreseeable misuse of it. Moreover, the vast number of characteristics to consider regarding a medical device, ranging from therapeutic area, types of devices, procedures and environments it will operate in, imposes an analysis framework that considers multiple factors in conjunction to make a benefit-risk evaluation. Hence, during the CYLCOMED project, a generalized benefit-risk framework was developed, and can be seen in Figure 4. It is composed of 6 phases: Therapeutic Context, Evaluation Criteria, Comparison Weights/Functions, Data Acquisition, Benefit-Risk Evaluation, and Sources of Uncertainties.

In the **Therapeutic Context** phase, the following activities are required:

- Analysis of the condition/disease, considering the nature of the disease, severity of the condition, unmet medical need and the intended population.
- Survey of the currently existing treatment.
- Analysis of applicable regulations, standards and laws.
- Determination of the key benefits and risks with the information compiled during the previous analysis.

In the **Evaluation Criteria** phase, the following activities are required:

- Definition of the factors to be considered (e.g., patients' quality of life, symptoms releave, operational impact) when analysing the key benefits and key risks.

In the **Comparison weights/Functions** phase, the following activities are required:

- Definition of the evaluation method. The evaluation method is represented as $b_{i,j}$ ($r_{k,l}$ functions and can yields quantitative, qualitative, or a combination of quantitative and qualitative scores.
- Then, it's important to define the way these evaluated benefits and risks are agglomerated until a final conclusion is reached.

In the **Data Acquisition** phase, the following activities are required:

- Definition of the evaluation data and data acquisition processes for the key benefits and risks. This can include, for example, expert groups opinions, clinical trials information or statistical data.
- These data will be used by the comparison functions, and ultimately, by the evaluation function.

In the **Benefit-Risk Evaluation** phase, the following activities are required:

- The benefit-risk evaluation will be determined from the evaluation function applied on the comparison functions and the acquired data.
- Further expert analysis may be required in order to interpret the result, and also to formally document the results.

Sources of Uncertainties include:

- Clinical relevance of key benefits and risks;

Funded by Horizon Europe Framework Programme of the European Union

- 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

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

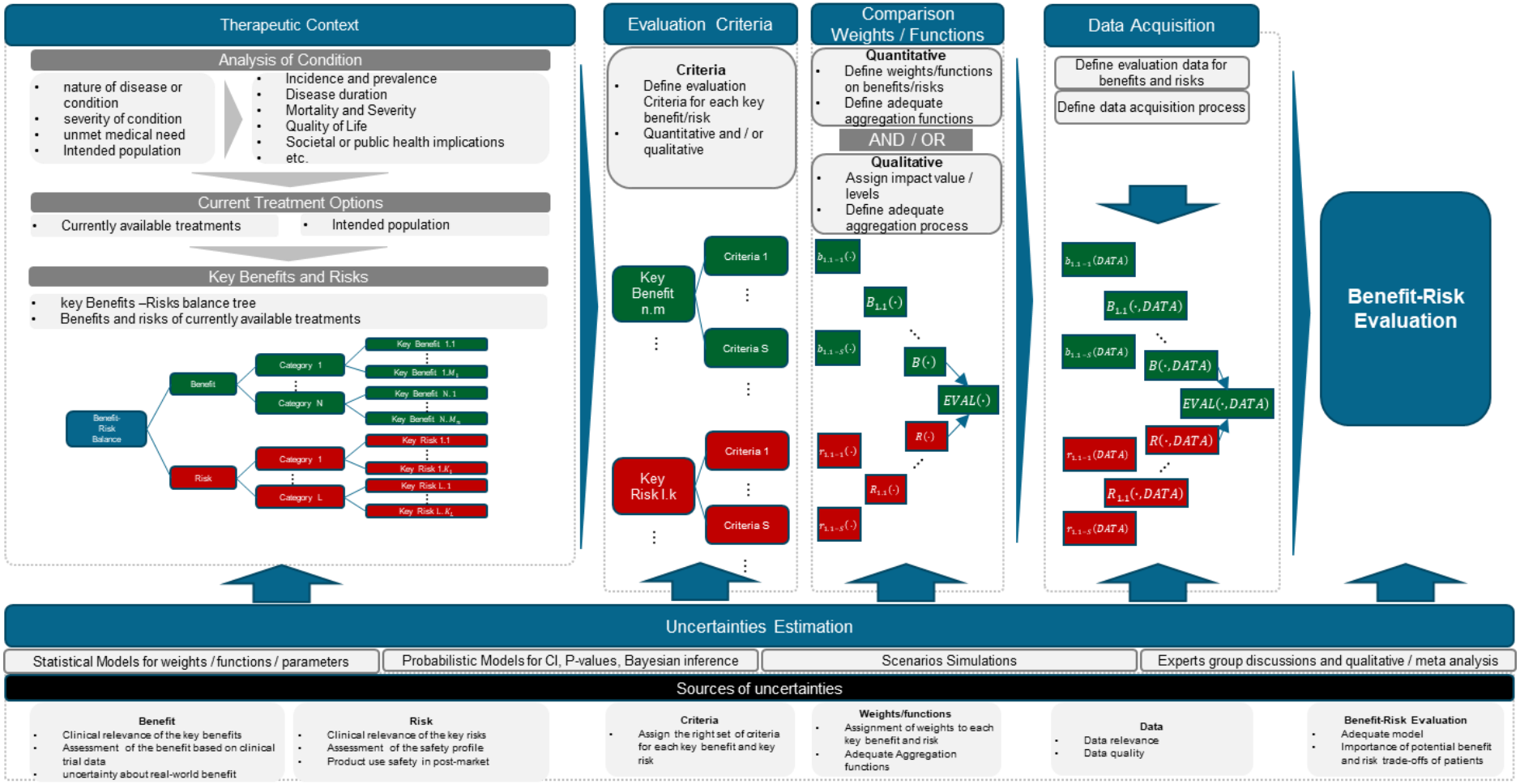

Figure 4 Benefit-Risk Scheme General View, from analysis performed on documents [8] and [9]

One of the best known approach is the Multi-Criteria Decision Approach (MCDA), which is a systematic decision-making framework that allows for multiple factors comparison. This method is employed in many contexts, and, in order to streamline the analysis of the cybersecurity of CMDs, which needs both the analysis from hospitals and manufacturers, MCDA seams the most effective and simple method to be used in the CYLCOMED project. As examples for factors to consider when defining the evaluation criteria, you can find in [10] a categorization of MCDA criteria, a result of the papers' systematic review they did on studies:

Table 3 MCDA criteria from [10]

Category	Key Terms Used
Health Outcomes and Benefits of Interventions	Health effects, quality of life, effectiveness, safety, complications, patient-reported outcomes
Type of Health Benefit	Individual vs public health benefits, public health interest, type of medical service
Impact of the Disease Targeted by Intervention	Severity of disease, size of affected population, number of beneficiaries, age group, socioeconomic impact, equity
Therapeutic Context of Intervention	Clinical guidelines, comparative intervention limitations, disease prevention potential
Economic Impact	Cost-effectiveness, total budget impact, affordability, marketability, impact on spending, ICER
Quality and Uncertainty of Evidence	Regulatory adherence, completeness of reporting, relevance and validity of data, evidence certainty
Implementation Complexity of Intervention	Technology applicability, system capacity, feasibility, technical complexity, variation in practice
Priorities, Fairness, and Ethics	Ethical acceptability, fairness, social/geographical equity, efficiency, priorities
Overall Context	Stakeholder pressure, political context, healthcare infrastructure impact, patient expectations

This method enables the analysis to be done quantitatively, qualitatively or with a mixture of both. For our purposes, in order to still be general enough to be used for any CMD, the CYLCOMED Benefit-Risk scheme will use the qualitative quantities.

The CYLCOMED project is focused on the trade-offs between cybersecurity and safety of patients. When performing a benefit-risk analysis, the cybersecurity will inevitably introduce benefits (e.g., more privacy, better access control mechanisms), but the overall functioning of the device could be worsened in some respects. These worsen aspects should be matched to the respective impacted benefits. Then, a qualitative analysis should be performed in order to understand if the implemented control will impact dramatically the benefits, and potentially outweigh them. After the considerations of all the benefit-risk matching is done, an overall evaluation is performed as to whether the CMD is considered safe and cyber-secure to be deployed.

In our context, we are analysing the impact that cybersecurity has on the CMD. To this end, we need to analyse the CMD, component by component, determine the threats it is exposed to, the vulnerabilities within the system, and then determine the cybersecurity controls to be

implemented on the device. These controls will impact the functionalities of the CMD, resulting in some negative impact on the CMD's benefits. Ultimately, these functionality impacts should be weighed against the benefits, resulting into a final decision as to whether the CMD is considered safe and cyber-secure. To further analyse the CMD, we propose the use of Data Flow Diagram decomposition to understand the data flow and storage components of the CMD, the Cyber Kill Chain for threat modelling and giving hints on what cybersecurity controls should be employed. Then, the cybersecurity controls should be selected, followed by functionality impact analysis to determine which benefits will be impacted, what hazards will be aggravated and which new hazards will emerge.

3.1 Date Flow Diagram Decomposition

A Data Flow Diagram decomposition is a structured modelling framework for decomposing systems into simpler components, functions and their communication pathways. It enables the visualization of data flows, and where they are stored, in a system. The DFD3 notation includes the following components (represented in

Figure 5) [11]:

External entities represent any system, device, or user outside the control of the system being modelled. These entities interact with the system, typically by sending or receiving data. Examples include [11]:

- Users: Patients, doctors, nurses, and hospital staff interacting with the device;
- Hospital Systems: Electronic Health Record (EHR) systems, Picture Archiving and Communication System (PACS);
- Mobile Apps: applications that sync data between the device and cloud;
- Cloud services: supporting services for patients;
- Third-Party Services: External cloud storage, external data analysis providers.

External entities can be attack entry points, e.g., can potentially be compromised and it falls outside the control of the system.

Data Storage are locations where information is stored. It includes databases, logs, temporary files. Examples include [11]:

- On-Device Storage: Wearable devices storing temporary patient data before transmission.
- Cloud Databases: Central storage for patient records.
- EHR Systems: Hospital databases storing patient history and scan images.
- Logs & Audit Trails: System logs tracking device activity and user access.

Data breaches, and data tampering can occur on these devices, to launch other attacks.

Processes include software functions, algorithms and system operations that process data. It includes [11]:

- Sensor Data Processing: A wearable device collects heart rate and processes the data,
- Data Encryption Module: Encrypting patient scan data before transmission,
- Authentication & Authorization Service: Verifies if a user or system has permission to access data;
- Data Analysis Algorithm: AI-powered prediction models analysing patient data for anomalies.

Funded by Horizon Europe Framework Programme of the European Union

Processes could be targeted as they are subject to malware injections, and they may also present vulnerabilities, like weak encryption, misconfigurations, or even be unpatched.

As attacks can take place where the algorithms are stored, we introduce, in the model, another component called the **Code Stores**, which are locations where algorithms are stored, updated and fetched from to be processed by the system. In this way, we can also model the attacks performed on code stores, when they are updated, for example.

Data flows represent communication channels between the modelled components and they captures all the data flowing in and out of every component. Examples include:

- Device to mobile app communication, through Bluetooth, USB, Wi-Fi;
- Mobile app to cloud services communication, through internet, API calls;
- Cloud to Hospital systems communication for database synchronization;
- Clinician's workstation to medical device communication, through USB, Bluetooth, Wi-Fi or network connection.

Unsecured data flows and lack of integrity checks are examples of vulnerabilities attackers could exploit.

Trust Boundaries define trusted and untrusted components, enabling the identification of what components lies within security zones, and what components lie outside of it. For example:

- Between the mobile phone and a medical device, the trusted zone could be delimited in the wireless connection (e.g., Bluetooth);
- Between the hospital network and the internet, the trusted zone could be delimited in the hospital's firewall devices.

Trust boundaries help identify security risks whenever there is data flow from one component to another. When boundaries are not well-identified, unauthorized access risks are more common to appear.

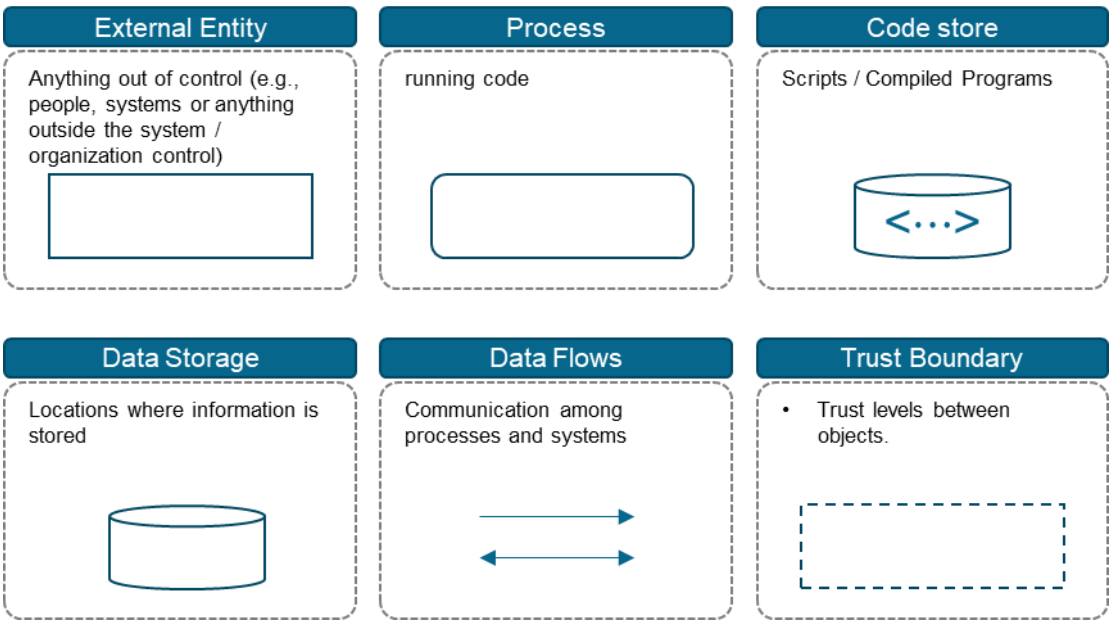

Figure 5 Data Flow Diagram icons and brief description

Funded by Horizon Europe Framework Programme of the European Union

3.2 Cyber Kill Chain

The Cyber Kill Chain is a framework developed by Lockheed Martin to identify and prevent cyber-attacks [12], [13]. This framework is structured in seven stages that adversaries must go through to successfully carry out an attack. Moreover, by preventing any of the stages progression, the "chain of attack" is broken, meaning that the cyber-attack is prevented. The seven stages are the following (see Figure 6):

- **Reconnaissance** – information gathering;
- **Weaponization** – attack tools preparation;
- **Delivery** – attack vector deployment;
- **Exploitation** – gain access to target system;
- **Installation** – persistence in target system(s);
- **Command and Control** – control target system remotely;
- **Actions on Objective** – attack execution.

In the **Reconnaissance** phase, the attacker's goal is to identify the weak points of the organization / system. Weak points could be system vulnerabilities, personnel. This is sometimes referred to as the primary target. Examples of primary targets include:

- Employees, who connects to organizations' internal systems, has authentication credentials;
- Public-facing systems (e.g., websites);
- Accessible devices (e.g., laptop, IoT device).

During this phase, the attacker will use one or more of the following tactics (non-exhaustive): IP scanning, public database search, social media analysis, phishing campaigns, scan internet for the system (systems) vulnerability (vulnerabilities). On the organizations' site, defensive tactics include monitoring and analysis of the organization's website visit logs and activities to detect suspicious activities, deployment of firewalls, Intrusion Detection Systems (IDS).

In the **Weaponization** phase, the attacker creates, acquires and/or modifies attack tools, such as malware or exploit kits. The intent is to explore vulnerabilities of the initial target and gain some level of control of a certain system. Defensive tactics for this phase include continuous intelligence gathering about attack tools to identify their trends, patterns and to deploy cybersecurity controls for detection and containment of such attack tools.

In the **Delivery** phase, the attacker conveys the malware or attack tool to the initial target. It can be conveyed via phishing emails, malicious websites or even infected USB drivers. Examples of delivery mechanisms to primary targets include:

- Phishing email with malicious attachment to targeted Employee;
- Compromise a website that the target employee visits often (Watering Hole Attack);
- Infected USB drive, left unattended in company premise, so that some employee picks it up and connects it to its' computer;
- Exploit directly the Public-facing system vulnerability with the attack tool.

Defenders can deploy email and attachment monitoring and security tools, sandboxing techniques, endpoint protection such as up-to-date antivirus.

During the **Exploitation** phase, the initial target's vulnerability is exploited. For example, a distracted employee clicks on the phishing email's attachment, or the public-facing system without up-to-date patching is exploited.

Defenders should conduct vulnerability scanning and regular patching of software, restrict administration privileges, software whitelisting and awareness training programs for employees.

Funded by Horizon Europe Framework Programme of the European Union

In the **Installation** phase, the attack tool runs the malicious code on the infected system. The main objective is to run commands, undetected, in order to maintain control over the infected system. These commands could enable backdoors installation, new access accounts creation, or start-up settings modifications which would enable the attacker to regain access to the system. In this way, the attacker has persistent access to the system, even if it's rebooted.

Defenders can deploy Host Intrusion Detection Systems (HIPS) to detect unauthorized installations, log monitor and analysis to detect strange activities, and monitor users' accounts and permissions.

During the **Command and Control** phase, the attacker connects to the infected system. The attacker now can exfiltrate data, access to credential data and try to make lateral movements (access other devices) until he gets to the primary target.

Defenders should monitor and analyze network traffic, looking for suspicious activities, limit systems' accesses (access control enforcement) or use multi-factor authentication mechanisms.

In the **Actions on Objective**, the attacker carries out the intended attack on the targeted system. The objective could be, for example, data theft, espionage or ransomware attack.

Defenders should have in place a Security Information and Event Management (SIEM) system and an incident response team ready to act upon detecting an incident.

Funded by Horizon Europe Framework Programme of the European Union

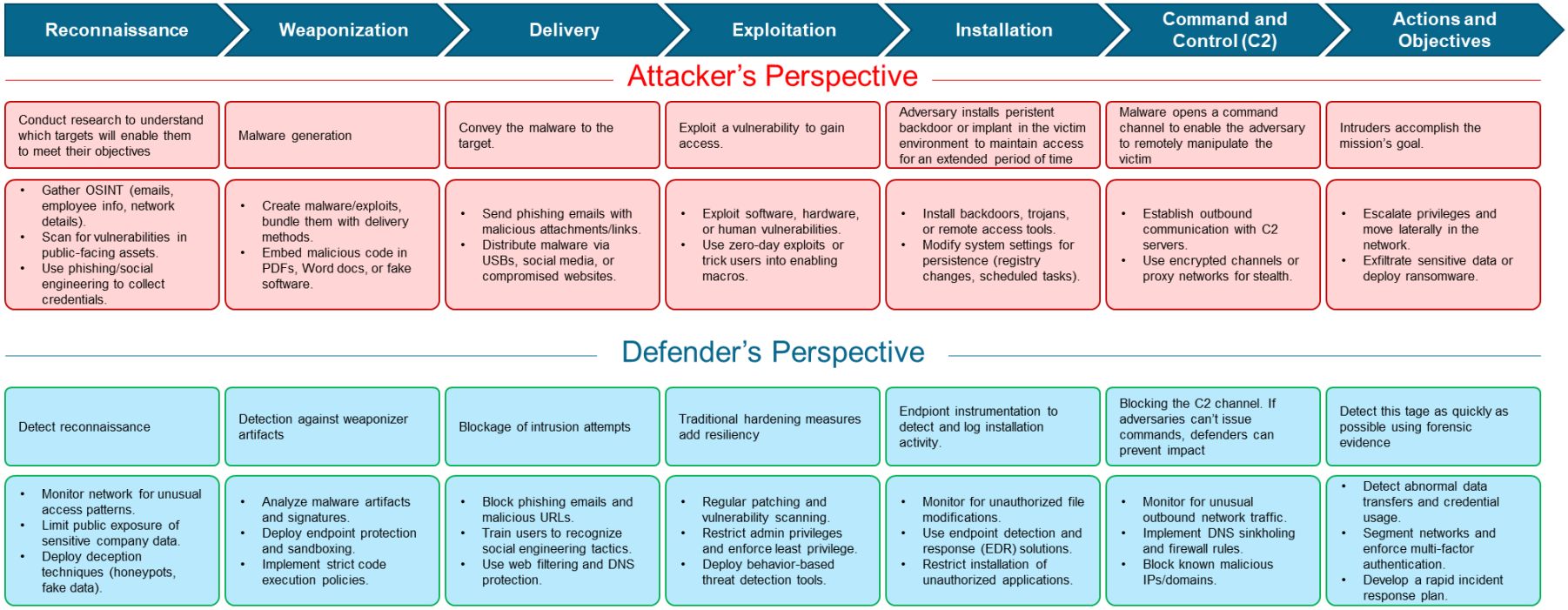

Figure 6 The cyberkill chain – description of the phases, the attack and defense objectives and respective actions

3.3 Cybersecurity Controls

In the CYLCOMED context, a CMD will be developed by the manufacturer, who can implement some cybersecurity controls in the system. Examples include technical controls for maintaining **confidentiality**, **integrity**, **availability** and **privacy** of the information directly in the CMD. **Access control mechanisms** (e.g., authentication, authorization) and **activity log** are other examples of such controls.

On the other hand, when the CMD is deployed in a hospital environment, the CMD cybersecurity controls must be integrated within its' own cybersecurity system. The CMD must be properly configured to function with the hospital systems, with logging information being fed to the hospitals' **monitoring and logging** systems, **access control mechanisms**, and **incident management team**. Also, information collected from the CMD should be properly managed to protect the patient's **privacy**. The hospital should contribute to the CMD enhancement through feedbacks about problems and improvements of the CMD.

The CMD can also be deployed on the patients' house, or even be a wearable. The patient should also follow the manufacturers' and the hospitals' guidance when configuring and using the CMD. The patient should follow good practices when using the access control mechanisms and should be familiar with the **CMD** alarms to confirm correct functioning. The patient should give feedback to the hospital and the manufacturer about any problems that the CMD has, to contribute to the continuous improvement of the CMD and the hospital cybersecurity system.

One aspect that needs to be highlighted is **data quality,** which is crucial within the healthcare sector. Diagnostics information, for example, must be kept up-to-date, complete and available whenever needed, to avoid safety risks. Several cybersecurity controls can be deployed to protect data quality, but some principles must be kept in mind when selecting them.

Above all the controls, a **governance structure** must be in place for managing and oversight of all the processes, procedures, policies, and any decision on what cybersecurity controls to implement, both in the manufacturers' site and the hospitals' site.

Taking all these aspects into consideration, the framework has cybersecurity controls organized in 10 functional categories, which helps understand how the cybersecurity of any device is managed (see Figure 7):

- **Governance** – high level management and strategic oversight of security policies, procedures and practices;
- **Confidentiality** – controls that ensure that sensitive information is accessed only by authorized entities;
- **Integrity** – controls to protect data from unauthorized or unintended modifications or destruction of data;
- **Availability** – controls to ensure timely and reliable access to information and systems for authorized entities;
- **Privacy** – controls intended to protect personal information according to laws and policies;
- **Data Quality** – controls that ensure data accuracy, completeness, reliability and consistency. This category is particularly important when using technologies such as AI (e.g., training the model, storing the model), and blockchain (e.g., guarantee that the information is correct);
- **Access Control** – controls to ensure only authorized entities access the systems, data or any resources. It enforces role-based access, authorizations and permissions to perform the appropriate functions;

- **Monitoring and Logging** – controls to ensure the process of collecting of relevant data, to ensure proper analysis and detection of security threats analysing and to ensure accountability;
- **Incident Management** – controls ensuring there is a process of detection, responding to, and recovery from security incidents effectively;
- **Continuous Improvement** – controls that ensure cybersecurity practices evolve to meet emerging threats and improve over time.

The cybersecurity controls from the NIST CSF 2, and clauses from ISO 27001 and ISO 14971 are mapped to these categories. We note that the controls from ISO 27001, Annex A, were not mapped here as there would be repetitions with NIST CSF 2 controls. Also, the controls are focused on cybersecurity and they should be viewed as controls to be implemented within a broader risk management process that includes the manufacturer, the hospital and the patient.

Table 4 Cybersecurity controls of NIST CSF2.0, ISO 27001 and ISO 14971 mapped to the 10 Categories of the CYLCOMED Risk Management Framework

CYLCOMED Framework Control Category	Control Category	Control / Category	Description
Governance	Organizational Context (GV.OC)	GV.OC-01	The organizational mission is understood and informs cybersecurity risk management
Governance	Organizational Context (GV.OC)	GV.OC-02	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered
Governance	Organizational Context (GV.OC)	GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed
Governance	Organizational Context (GV.OC)	GV.OC-04	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated
Governance	Organizational Context (GV.OC)	GV.OC-05	Outcomes, capabilities, and services that the organization depends on are understood and communicated
Governance	Risk Management Strategy (GV.RM)	GV.RM-01	Risk management objectives are established and agreed tby organizational stakeholders
Governance	Risk Management Strategy (GV.RM)	GV.RM-02	Risk appetite and risk tolerance statements are established, communicated, and maintained
Governance	Risk Management Strategy (GV.RM)	GV.RM-03	Cybersecurity risk management activities and outcomes are included in enterprise risk management processes
Governance	Risk Management Strategy (GV.RM)	GV.RM-04	Strategic direction that describes appropriate risk response options is established and communicated
Governance	Risk Management Strategy (GV.RM)	GV.RM-05	Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties

Funded by Horizon Europe Framework Programme of the European Union

CYLCOMED Framework Control Category	Control Category	Control / Category	Description
	Risk Management Strategy (GV.RM)	GV.RM-06	A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated
Governance	Risk Management Strategy (GV.RM)	GV.RM-07	Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions
Governance	Roles, Responsibilities, and Authorities (GV.RR)	GV.RR-01	Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving
Governance	Roles, Responsibilities, and Authorities (GV.RR)	GV.RR-02	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced
Governance	Roles, Responsibilities, and Authorities (GV.RR)	GV.RR-03	Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies
Governance	Roles, Responsibilities, and Authorities (GV.RR)	GV.RR-04	Cybersecurity is included in human resources practices
Governance	Policy (GV.PO)	GV.PO-01	Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced
Governance	Policy (GV.PO)	GV.PO-02	Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes
Governance	Oversight (GV.OV)	GV.OV-01	Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction
Governance	Oversight (GV.OV)	GV.OV-02	The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks
Governance	Oversight (GV.OV)	GV.OV-03	Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed
Governance	Cybersecurity Supply Chain Risk Management (GV.SC)	GV.SC-01	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders
Governance	Cybersecurity Supply Chain Risk Management (GV.SC)	GV.SC-02	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally

Funded by Horizon Europe Framework Programme of the European Union

CYLCOMED Framework Control Category	Control Category	Control / Category	Description
Governance	Cybersecurity Supply Chain Risk Management (GV.SC)	GV.SC-03	Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes
Governance	Cybersecurity Supply Chain Risk Management (GV.SC)	GV.SC-04	Suppliers are known and prioritized by criticality
Governance	Cybersecurity Supply Chain Risk Management (GV.SC)	GV.SC-05	Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties
Governance	Cybersecurity Supply Chain Risk Management (GV.SC)	GV.SC-06	Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships
Governance	Cybersecurity Supply Chain Risk Management (GV.SC)	GV.SC-07	The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship
Governance	Cybersecurity Supply Chain Risk Management (GV.SC)	GV.SC-08	Relevant suppliers and other third parties are included in incident planning, response, and recovery activities
Governance	Cybersecurity Supply Chain Risk Management (GV.SC)	GV.SC-09	Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle
Governance	Cybersecurity Supply Chain Risk Management (GV.SC)	GV.SC-10	Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement
Access Control	Identity Management, Authentication, and Access Control (PR.AA)	PR.AA-01	Identities and credentials for authorized users, services, and hardware are managed by the organization
Access Control	Identity Management, Authentication, and Access Control (PR.AA)	PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions
Access Control	Identity Management, Authentication,	PR.AA-03	Users, services, and hardware are authenticated

Funded by Horizon Europe Framework Programme of the European Union

CYLCOMED Framework Control Category	Control Category	Control / Category	Description
	and Access Control (PR.AA)		
Access Control	Identity Management, Authentication, and Access Control (PR.AA)	PR.AA-04	Identity assertions are protected, conveyed, and verified
Access Control	Identity Management, Authentication, and Access Control (PR.AA)	PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties
Access Control	Identity Management, Authentication, and Access Control (PR.AA)	PR.AA-06	Physical access to assets is managed, monitored, and enforced commensurate with risk
Governance	Awareness and Training (PR.AT)	PR.AT-01	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind
Governance	Awareness and Training (PR.AT)	PR.AT-02	Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind
Confidentiality, Integrity, Availability, Privacy	Data Security (PR.DS)	PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected
Confidentiality, Integrity, Availability, Privacy	Data Security (PR.DS)	PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected
Confidentiality, Integrity, Availability, Privacy	Data Security (PR.DS)	PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected
Availability, Incident Management	Data Security (PR.DS)	PR.DS-11	Backups of data are created, protected, maintained, and tested
Governance	Platform Security (PR.PS)	PR.PS-01	Configuration management practices are established and applied
Access Control, Integrity, Availability, Data Quality	Platform Security (PR.PS)	PR.PS-02	Software is maintained, replaced, and removed commensurate with risk
Access Control	Platform Security (PR.PS)	PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk

Funded by Horizon Europe Framework Programme of the European Union

CYLCOMED Framework Control Category	Control Category	Control / Category	Description
Monitoring and Logging, Data Quality	Platform Security (PR.PS)	PR.PS-04	Log records are generated and made available for continuous monitoring
Access Control, Integrity, Data Quality	Platform Security (PR.PS)	PR.PS-05	Installation and execution of unauthorized software are prevented
Governance	Platform Security (PR.PS)	PR.PS-06	Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle
Access Control	Technology Infrastructure Resilience (PR.IR)	PR.IR-01	Networks and environments are protected from unauthorized logical access and usage
Integrity, Availability, Data Quality	Technology Infrastructure Resilience (PR.IR)	PR.IR-02	The organization's technology assets are protected from environmental threats
Availability, Incident Management	Technology Infrastructure Resilience (PR.IR)	PR.IR-03	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations
Availability, Incident Management	Technology Infrastructure Resilience (PR.IR)	PR.IR-04	Adequate resource capacity to ensure availability is maintained
Logging and Monitoring	Continuous Monitoring (DE.CM)	DE.CM-01	Networks and network services are monitored to find potentially adverse events
Logging and Monitoring	Continuous Monitoring (DE.CM)	DE.CM-02	The physical environment is monitored to find potentially adverse events
Logging and Monitoring	Continuous Monitoring (DE.CM)	DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events
Logging and Monitoring	Continuous Monitoring (DE.CM)	DE.CM-06	External service provider activities and services are monitored to find potentially adverse events
Logging and Monitoring	Continuous Monitoring (DE.CM)	DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events
Incident Management	Adverse Event Analysis (DE.AE)	DE.AE-02	Potentially adverse events are analysed to better understand associated activities
Incident Management	Adverse Event Analysis (DE.AE)	DE.AE-03	Information is correlated from multiple sources
Incident Management	Adverse Event Analysis (DE.AE)	DE.AE-04	The estimated impact and scope of adverse events are understood
Incident Management	Adverse Event Analysis (DE.AE)	DE.AE-06	Information on adverse events is provided to authorized staff and tools
Incident Management	Adverse Event Analysis (DE.AE)	DE.AE-07	Cyber threat intelligence and other contextual information are integrated into the analysis
Incident Management	Adverse Event Analysis (DE.AE)	DE.AE-08	Incidents are declared when adverse events meet the defined incident criteria

Funded by Horizon Europe Framework Programme of the European Union

CYLCOMED Framework Control Category	Control Category	Control / Category	Description
Incident Management	Incident Management (RS.MA)	RS.MA-01	The incident response plan is executed in coordination with relevant third parties once an incident is declared
Incident Management	Incident Management (RS.MA)	RS.MA-02	Incident reports are triaged and validated
Incident Management	Incident Management (RS.MA)	RS.MA-03	Incidents are categorized and prioritized
Incident Management	Incident Management (RS.MA)	RS.MA-04	Incidents are escalated or elevated as needed
Incident Management	Incident Management (RS.MA)	RS.MA-05	The criteria for initiating incident recovery are applied
Incident Management	Incident Analysis (RS.AN)	RS.AN-03	Analysis is performed to establish what has taken place during an incident and the root cause of the incident
Incident Management	Incident Analysis (RS.AN)	RS.AN-06	Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved
Incident Management	Incident Analysis (RS.AN)	RS.AN-07	Incident data and metadata are collected, and their integrity and provenance are preserved
Incident Management	Incident Analysis (RS.AN)	RS.AN-08	An incident's magnitude is estimated and validated
Incident Management	Incident Response Reporting and Communication (RS.CO)	RS.CO-02	Internal and external stakeholders are notified of incidents
Incident Management	Incident Response Reporting and Communication (RS.CO)	RS.CO-03	Information is shared with designated internal and external stakeholders
Incident Management	Incident Mitigation (RS.MI)	RS.MI-01	Incidents are contained
Incident Management	Incident Mitigation (RS.MI)	RS.MI-02	Incidents are eradicated
Incident Management	Incident Recovery Plan Execution (RC.RP)	RC.RP-01	The recovery portion of the incident response plan is executed once initiated from the incident response process
Incident Management	Incident Recovery Plan	RC.RP-02	Recovery actions are selected, scoped, prioritized, and performed

Funded by Horizon Europe Framework Programme of the European Union

CYLCOMED Framework Control Category	Control Category	Control / Category	Description
	Execution (RC.RP)		
Incident Management	Incident Recovery Plan Execution (RC.RP)	RC.RP-03	The integrity of backups and other restoration assets is verified before using them for restoration
Incident Management	Incident Recovery Plan Execution (RC.RP)	RC.RP-04	Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms
Incident Management	Incident Recovery Plan Execution (RC.RP)	RC.RP-05	The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed
Incident Management	Incident Recovery Plan Execution (RC.RP)	RC.RP-06	The end of incident recovery is declared based on criteria, and incident-related documentation is completed
Incident Management	Incident Recovery Communication (RC.CO)	RC.CO-03	Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders
Incident Management	Incident Recovery Communication (RC.CO)	RC.CO-04	Public updates on incident recovery are shared using approved methods and messaging
Continuous Improvement	Monitor and Review the ISMS	Clause 9 (ISO 27001)	Monitor, analyse and evaluate the ISMS
Continuous Improvement	Monitor and Review the ISMS	Clause 9 (ISO 27001)	Conduct internal audits
Continuous Improvement	Monitor and Review the ISMS	Clause 9 (ISO 27001)	Management reviews of ISMS
Continuous Improvement	Improvement	Clause 10 (ISO 27001)	Improvements must be made taking corrective actions
Continuous Improvement	Improvement	Clause 10 (ISO 27001)	Continual improvement processes must be implemented
Continuous Improvement	Production and Post-Production activities	Clause 10 (ISO 14971)	Establishment of system to collect and review relevant information regarding production and post-production of MD
Continuous Improvement	Production and Post-Production activities	Clause 10 (ISO 14971)	Corrective actions on the MD's life cycle if new risks/hazards are discovered

Funded by Horizon Europe Framework Programme of the European Union

Considering the asset to be the CMD, the controls from the 10 categories must be implemented/followed by the manufacturer, the healthcare provider and the patient. Consider, for example, the use of authentication and encryption technologies. The Manufacturer should implement such mechanisms in the CMD, but the Healthcare provider should be the one managing the encryption keys if the CMD communicates directly to their facilities. Moreover, the patient should follow cybersecurity hygiene in order to use those mechanisms properly, as to prevent attackers from getting his credentials. Moreover, logging capabilities can be implemented in the CMD, but the Healthcare provider should have an incident management team, capable of analysing the logs generated by the CMD, and to act upon a detected incident. The patient could have some mechanism to check if the CMD is functioning properly with an adequate alarming system and with the information from the CMD's user guide.

Moreover, this framework is general enough to be used for asset classes encompassing cloud infrastructures, AI models, AI data, blockchain, any IoT device, any type of network element (including 5G). Please refer to Annexes A through E for more information on the vulnerabilities, threats and countermeasures for these technologies.

Funded by Horizon Europe Framework Programme of the European Union

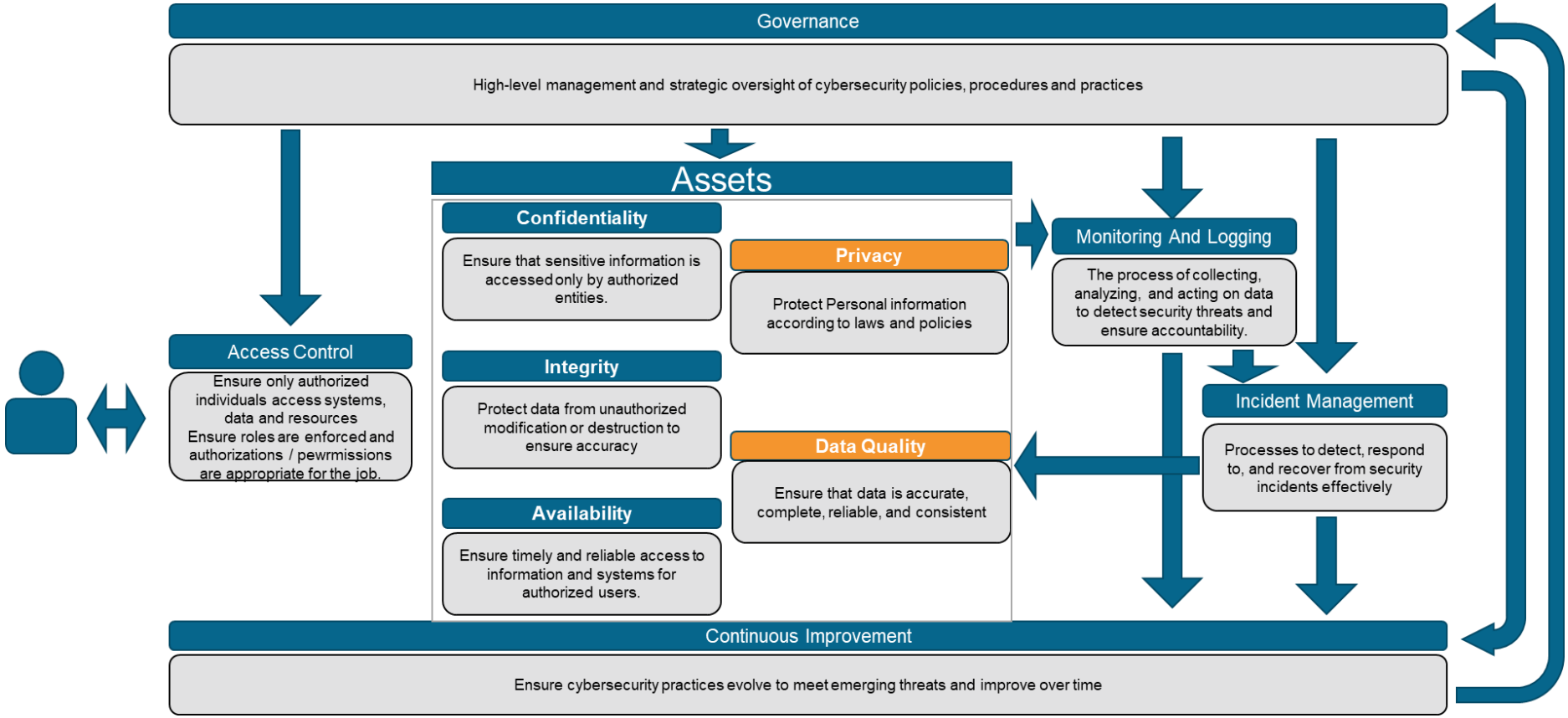

Figure 7 The relation between the asset (e.g., CMD, data storage, data at rest) and the 10 cybersecurity control categories of the CYLCOMED Risk Management Framework

3.4 Device Characteristics for Evaluating Benefits and Risks of a CMD

The ISO/IEC 20141:2024 standard provides a standardized reference architecture for IoT devices [14]. It describes several architecture views to suit several types of stakeholders, like project managers, IoT experts or system architects. It includes:

- Foundational IoT viewpoint;
- Business viewpoint;
- Usage viewpoint;
- Functional viewpoint;
- Trustworthiness viewpoint;
- Construction viewpoint.

For evaluating a CMD with regards to the benefits and risks, there are several aspects, drawn from the different viewpoints, that should be considered. Here is a compilation from a broader list of aspects from the standard, and depicted in Figure 8.

Internal Functional Model:

- Data functions – functions for controlling, managing and analysing data;
- Control functions – functions that enable sending commands to the system;
- Analysis function – include analytics, cognitive, streaming data, visualization, business rules and application logic services;
- Data Management functions – includes data transformation, filtering, cleaning, ELT (extract, transform, load), rules and notifications, device data store, analytics data store, and historical data store functions;
- Management functions – functions like provisioning, monitoring, reporting, interaction between components, policy management, service automation, service level management, service catalogues, device registries, device management, account management, subscription management, billing accounts;
- Communication function – include data transfer, network interface, and application interface functions
- Resilience Function – functions enabling recovery to operational condition quickly following an incident. It is related to concepts like self-healing, self-configuring, self-organizing, and self-protecting.
- Reliability Function – functions that ensure that the IoT system / component can perform its required functions under predefined conditions for a specified time;

Trustworthiness:

- Resilience Function – same as defined in internal functional model;
- Reliability Function – same as defined in internal functional model;
- Compliance – refers to compliance to rules defined by law, regulation, standards or policies.

Usage View:

- Sense function – environmental sensing and data reading capabilities;
- Actuate function – capabilities for acting on the environment when receiving control signals;

- Digital interface – includes APIs for any “digital” user (person or machine);
- Human interface – includes access portals, or user interface for people;

The standard also includes, in the Trustworthiness viewpoint, the confidentiality, integrity, availability and safety characteristics. These characteristics, in our setting, should be evaluated taking into account the former ones.

When projecting the CMD, the characteristics will need to be specified in order to evaluate if the benefits can be attained. For example, if sensors have some delays, it might be detrimental or negligible for the patient, depending on the treatment. When introducing cybersecurity controls, delays on some functions, like sensor delays, actuators delays, or even more complicated human interfaces might hinder the device’s correct use.

Characterizing the metrics for the medical device enables the evaluation of the impact of cybersecurity controls on hazards and benefits, when considering the correct use and the foreseeable misuse of the device.

Funded by Horizon Europe Framework Programme of the European Union

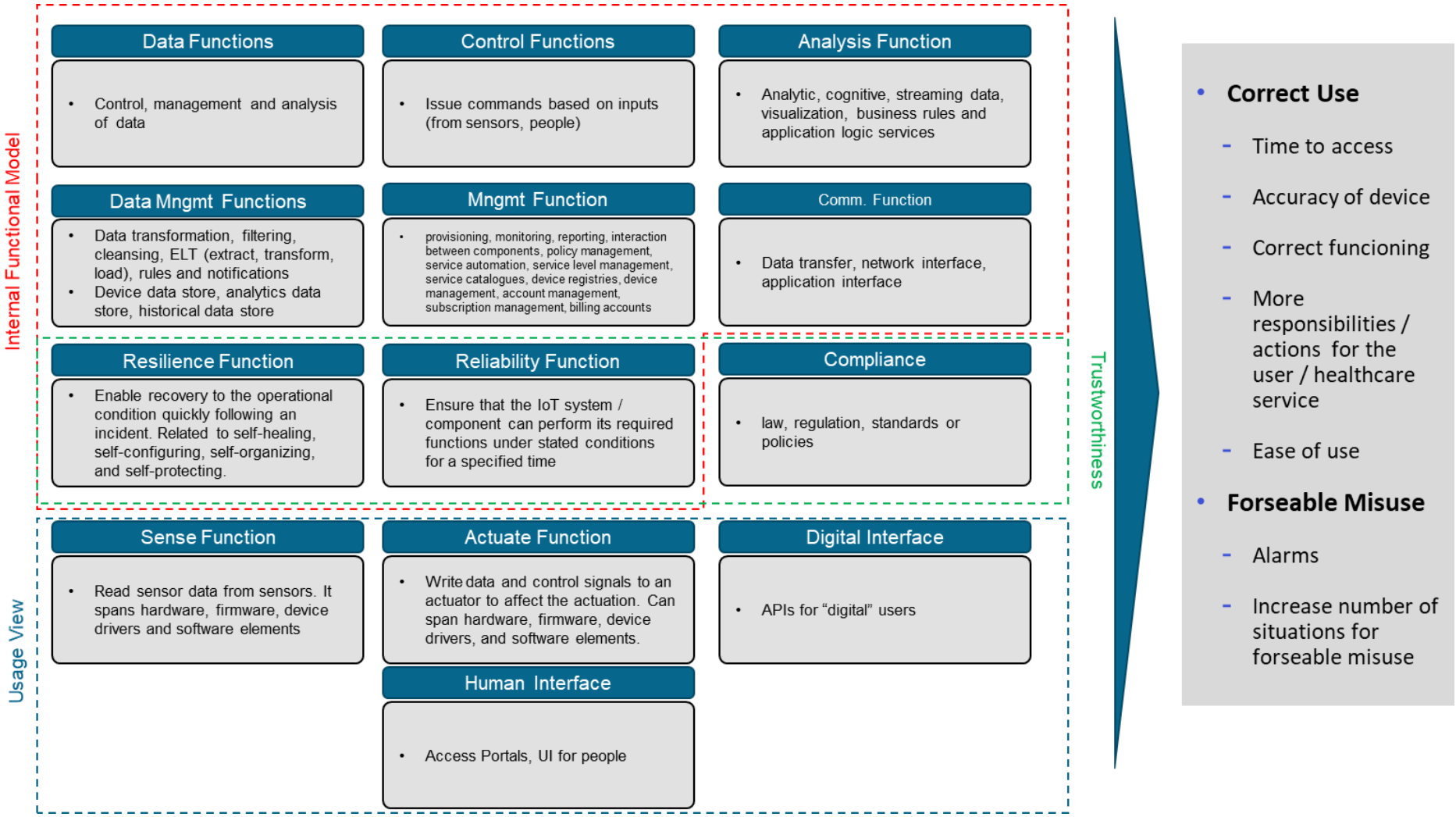

Figure 8 Functionalities of the CMD to take into account to evaluate the cybersecurity controls impact on the the correct use and foreseeable misuse of the CMD to predict the risks and impacts do benefits

4 Risk management of medical devices

CMDs can serve multiple purposes, ranging from implantable devices (e.g., Cardioverter Defibrillator, insulin pump, automated external defibrillator, pacemakers), Wearables (e.g., glucose monitor, fitness), and On-site equipment (e.g., X-ray machines, MRI, PACS, home haemodialysis equipment) [15], [16]. CMDs are characterized by their healthcare benefits, as well as its connectivity capabilities. Non-the-less, connectivity also introduces risks.

The risks can range from device related risks, networking related risks and data storage and analysis related risks [15]:

- Device related risks include resource limitation, heterogeneous technologies, authentication management, no embedded security support;
- Networking related risks include diversity of connection protocols, lack of end to end encryption, network latency;
- Data storage and analysis related risks include data at rest confidentiality violation, access control violations, no threat management.

Generally speaking, CMDs can be deployed on the patient (implantable, wearables), at home (haemodialysis) or at hospital premises. This imposes some shared responsibilities when it comes to maintaining a minimum level of cybersecurity to guarantee safety, confidentiality, integrity and availability of the device and their surrounding equipment / infrastructure.

The manufacturer should guarantee that the CMD has the required cybersecurity controls implemented/embedded in the device for guaranteeing the correct and safe use, such as up-to-date encryption algorithms, authentication mechanisms, proper logging mechanisms.

The Hospitals, on the other hand, needs to guarantee the whole infrastructure cybersecurity, meaning that, apart from the CMDs correct configuration and use, the hospitals must have in place other security measures, such as proper segmentation of networks, security patching updates for all the devices, access control mechanisms or cybersecurity awareness training.

Moreover, the patient also needs to guarantee that he enables the CMD's security features properly, follows the cybersecurity hygiene procedures (at home or at hospital) and also respects the Hospitals cybersecurity policies/processes.

4.1.1 Manufacturers' perspective

From the manufacturers' perspective, the CMD should have in place a risk management process for the device's lifecycle. The standard ISO 14971, together with the amendment A11:2021, Annexes Z, cover the MDR and IVDR regulations [17], [18] which should be followed by manufacturers selling their CMD within the EU. Figure 9 depicts the ISO 14971 standard.

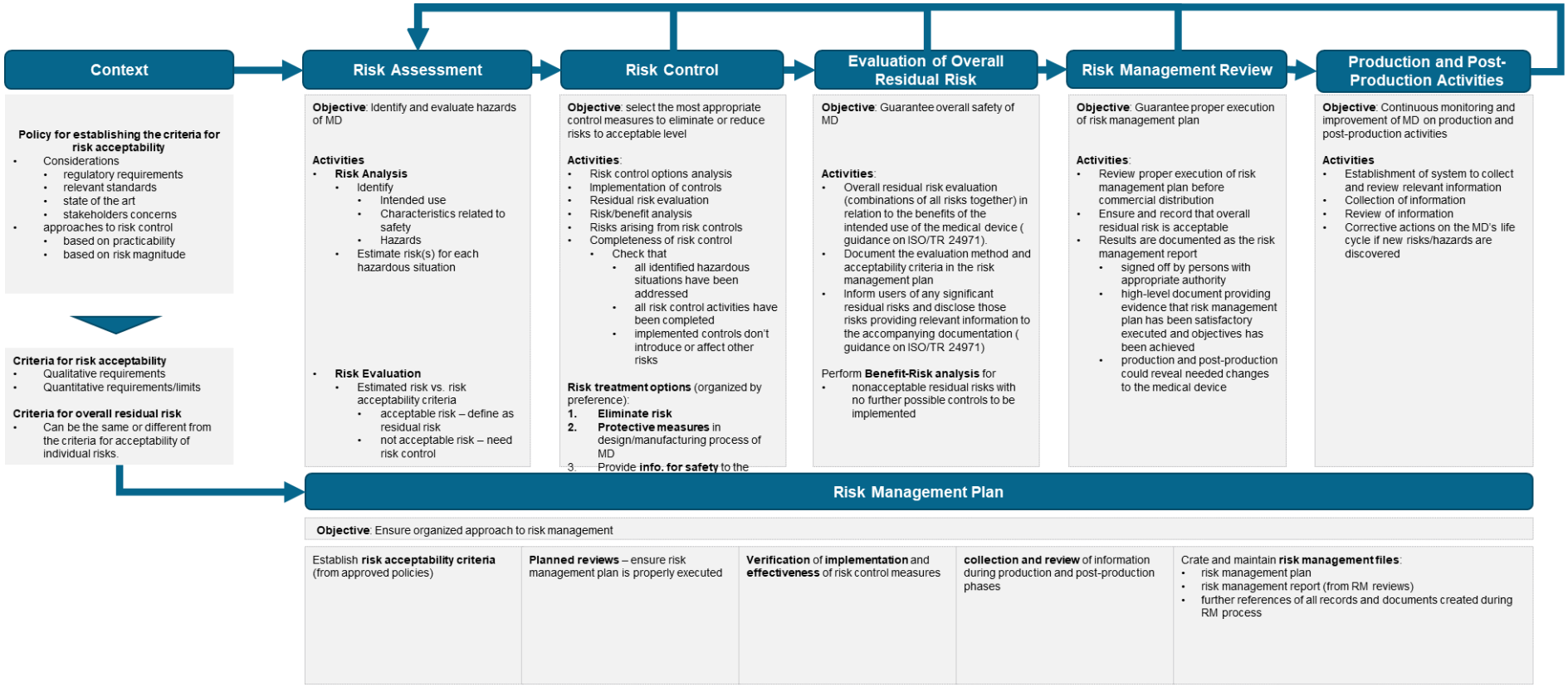

Figure 9 ISO 14971 Risk management process

It starts with determining the **context**, where the organization needs to understand and define the regulation requirements, approaches to risks, and address stakeholders' concerns. The risk acceptability criteria and overall residual risk criteria (after applying mitigation controls) must be defined as well. Also important is the definition of the benefits of the CMD.

Then, the **Risk Assessment** activities begin. The hazards / risk of the CMD is identified and the analysis and evaluation is performed.

According to the identified risks, the controls are selected, during the **Risk Controls** activities, to reduce risks to an acceptable level. The risk treatment options are the following (organized by preferences):

1. Eliminate the risk;
2. Protective measures in the design/manufacturing process of the medical device;
3. Provision of information for safety to the users.

Then, in order to perform the **Evaluation of the Overall Residual Risk** activities, where risks are combined in a logical way in order to understand if the compounded risk is acceptable or not. A benefit-risk analysis is performed to the residual risks that are not acceptable.

Next, during the **Risk Management Review** activities, a review of the process is made, in order to guarantee that the execution of the risk management was done according to plan.

The **Production and Post-Production Activities** aims at guaranteeing a continuous monitoring and improvement of the MD.

All the activities are supported by the **Risk Management Plan**, and all activities contribute to the risk management plan as well, updating documents, changing the plan when needed, keeping track of decisions and approvals.

Note that each of the activities, from Risk Control until Production and Post-Production activities all the activities have a feedback loop to the risk assessment activities. For example, by implementing risk control measures, new risks can emerge and should be assessed. During the Evaluation of Overall Residual Risks activities, unnacceptable residual risks might emerge, and further understanding of the risk and controls to be implemented migh be necessary. During production, new unforeseen risks should be assessed and new risk controls will need to be considered.

4.1.2 Healthcare Providers' perspective

From the healthcare providers' perspective, patient safety, and overall infrastructure cybersecurity must be protected. They usually follow, either national cybersecurity risk management references, or they follow well-established frameworks, such as ISO 27001, ISO 27002, ISO 27701, ISO 27005, ISO 31000, NIST Risk Management Framework, NIST Cybersecurity Framework, to name a few.

According to ISO 27005 (see Figure 10), the organization's risk management process, the first step is to **establish the organization's context**. In this stage, the organization:

- Determines who are the key stakeholders, the staff, roles and responsibilities, available resources;
- Determines the organization's governance model;
- Establishes the criteria to evaluate risks (factors to be considered);
- Establishes the impact criteria (how to evaluate the severity of the risk);

- Establishes the risk acceptance criteria.

Then, the next step is to **Identify Risk**, where the organization:

- Identifies the critical assets;
- Identifies existing vulnerabilities, threats and implemented controls;
- Identifies the risks to each asset.

In the **Risk Analysis** phase, estimation of the impact and likelihood of the risks follows, determining the risk levels of each risk.

In the **Risk Evaluation** phase, the risks determined in the risk analysis phase is contrasted with the risk evaluation criteria to determine with risks are acceptable and which are not. Risks are prioritized according to their risk scores.

In the **Risk Treatment** phase, the decision of avoiding, accepting, mitigating or transferring the risks is made. Cybersecurity controls belong to the mitigation action.

All the phases produce information that should be recorded.

This process flow is also supported by consultation with other sources of information and the results are communicated within the organization.

Also, monitoring and review mechanisms should be deployed to understand the effectiveness of the processes and the overall risk management.

Funded by Horizon Europe Framework Programme of the European Union

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

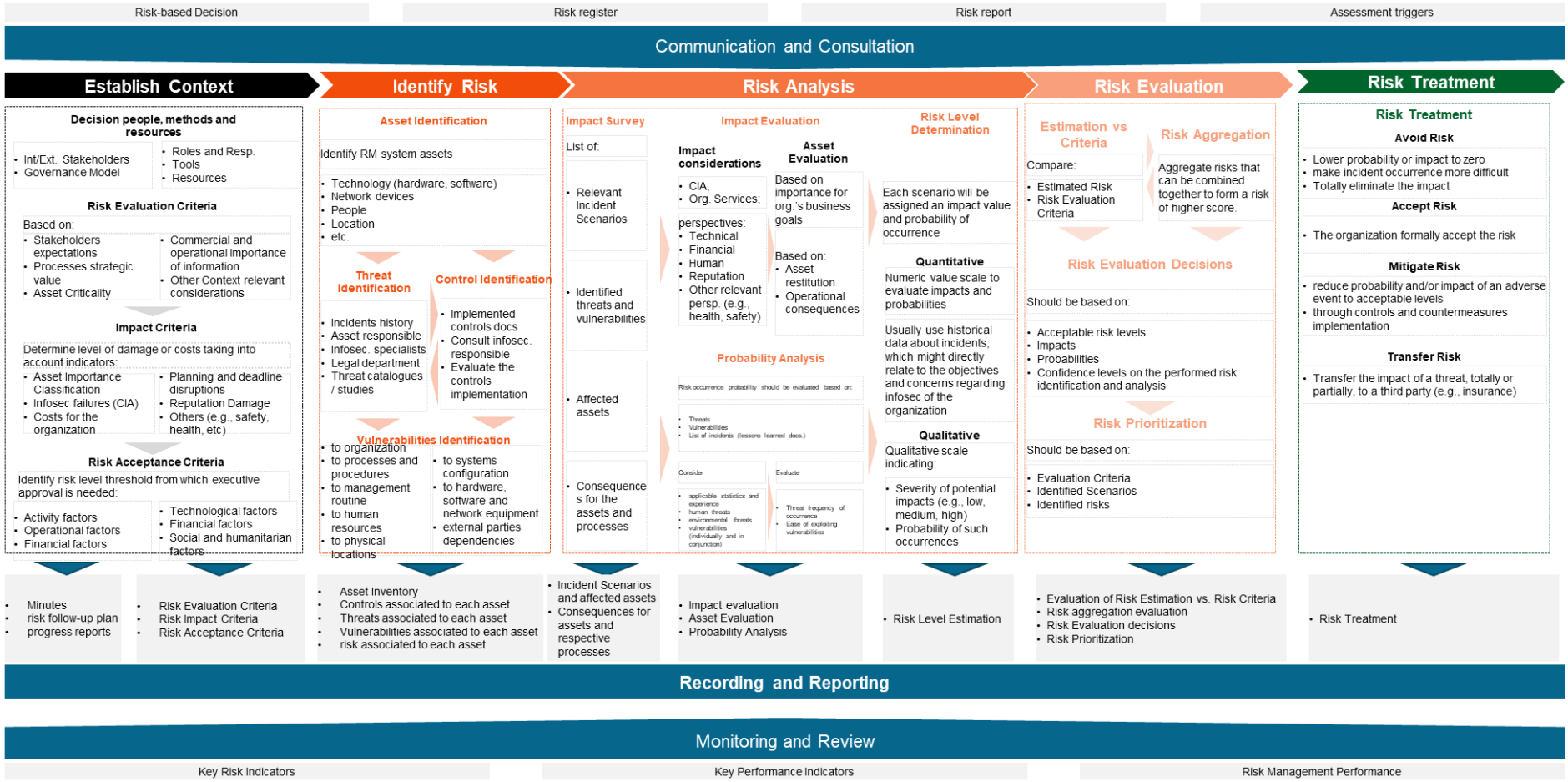

Figure 10 Cybersecurity Risk Management Framework process flow derived from the ISO 27005, based on the information in [3].

4.1.3 Patients' perspective

From the patients' perspective, the patient needs to follow the manufacturer's instructions and good practices in order to guarantee proper and safe use of the device.

Basic cybersecurity knowledge is preferable. Simple instructions onto how to setup the device and use the device's inbuilt cybersecurity controls should be given to the patient.

Also, when using the CMD in a hospital, the patient should follow the hospital's guidance and instructions in order to guarantee, not only his safety, but also to protect the hospital's infrastructure, in order to prevent any attacks from CMD misuse.

4.2 CYLCOMED Cybersecurity Risk Management Framework

The CYLCOMED Cybersecurity Risk Management Framework takes into account the manufacturers' cybersecurity risk management framework, the Hospital risk management and the patients' perspective as well.

At the centre of the framework lies the CMD. As per ISO 14971, and consequently, MDR and IVDR, the CMD must have countermeasures, or controls, to all the identified hazardous situations. This includes all the cybersecurity controls that the manufacturer can integrate into the device, as well as recommendations for those hazardous situations where there are no possible controls to be implemented.

Cybersecurity controls, like encryption algorithms or authentication mechanisms, needs to be well configured and used by hospitals and patients. In this sense, part of the responsibility of maintaining a minimum level of cybersecurity lies within the patients and the hospital staff.

Moreover, hospitals must have a cybersecurity system in place to secure the whole infrastructure, including controls such as network segmentation to contain any form of attack attempt from any device, including CMDs. Moreover, monitoring systems should also be in place to detect such attempts. With this regard, CMD alerts (e.g., log information), which are also defined by the manufacturer, needs to be used by the hospitals, and not by the manufacturer, to oversee hostile activities within the hospitals' infrastructures.

Note that the shared responsibility model is not new to cybersecurity and it is well established when using cloud services.

4.2.1 Principles and Characteristics for Cybersecurity, Privacy and Data Quality

Cybersecurity risk management frameworks have in them a set of principles that are embedded in them. Moreover, privacy risk management frameworks also follow a set of principles of their own. For example, security-by-design and privacy-by-design are usually described as controls to be applied, Other examples include the separation of duty principle / control, which should be used when defining the organization's cybersecurity roles, and the separation of privileges principle / control, which needs to be followed when defining and implementing access control mechanisms.

Both cybersecurity and privacy frameworks also have considerations related to data quality, although not explicitly. For example, by enforcing data confidentiality, integrity and availability, we are guaranteeing some principles of data quality like availability, accuracy, completeness,

and consistency. Moreover, by enforcing users' privacy rights like accuracy and quality, we are also guaranteeing data quality principles as well.

On the other hand, AI systems are highly reliant on the quality of data that are used to train them, ultimately having implications in the safety of the AI system. Data poisoning (please refer to Appendix E) is a serious risk that is directly linked to data quality. Data quality is also very relevant in software and virtualized environments, were every information has to be up-to-date, relevant in the context of use and complete.

The CYLCOMED Cybersecurity framework detached cybersecurity, privacy and data quality principles from the cybersecurity controls in order to server as a guidance for implementing the needed controls. Generally, principles cannot be directly verified. For example, considering that « Security-by-design« was applied means that, for example, encryption and authentication controls were considered right at the begining of the design of the system and they were implemented. The controls that you can audit are that « Security-by-Design« is stated in some cybersecurity policy, and that the controls were implemented.

In this document, you can find a compilation of cybersecurity, privacy and ata quality principles summarized in the following tables:

- Table 5 Cybersecurity principles from CyBok.
- Table 6 Cybersecurity principles from ISO 27701 related to privacy;
- [19]Table 7 Data Quality Characteristics from ISO/IEC 25012 :2008 – Data Quality Model [19].

Table 5 Cybersecurity principles from CyBok

Cybersecurity Principles	Description
Economy of Mechanism	Security controls should be as simple as possible to ensure high assurance.
Fail-Safe Defaults	Access should be denied by default and only granted explicitly.
Complete Mediation	Every access to every resource must be checked for authorization.
Open Design	Security should not rely on secrecy of design but on well-defined secrets.
Separation of Privilege	Require multiple independent conditions for authorization.
Least Privilege	Users and processes should operate with the minimum necessary permissions.
Least Common Mechanism	Minimize shared system components to reduce attack surfaces.
Psychological Acceptability	Security controls should be user-friendly to encourage correct usage.
Work Factor	Security controls should require more effort to bypass than an attacker can afford.

Funded by Horizon Europe Framework Programme of the European Union

Cybersecurity Principles	Description
Compromise Recording	Reliable records/logs should be used to detect security breaches.
Clear Abstraction, Modularity, and Layering	Systems should be designed with modularity and clear separations.
Partially Ordered Dependencies	Minimize dependencies to reduce cascading failures.
Secure Evolvability	Security mechanisms should allow updates to accommodate emerging threats.
Least Common Mechanism	Limit shared system components to reduce risks.
Efficiently Mediated Access	Ensure security checks do not impose excessive performance overhead.
Minimized Sharing	Restrict unnecessary sharing of resources.
Minimized Security Elements	Reduce the number of security components to improve assurance.
Reduced Complexity	Keep security implementations simple and structured.
Hierarchical Trust	Security failures in lower components should not compromise the system.
Inverse Modification Threshold	Most critical components should have the highest protection.
Hierarchical Protection	Most critical components should have the highest protection.
Trusted Communication Channels	Secure communication protocols must be used to prevent eavesdropping.
Secure Distributed Composition	Systems that enforce the same policy should maintain security when integrated.
Self-Reliant Trustworthiness	A system should remain secure even when disconnected from external sources.
Economic Security	Security measures should be cost-effective and feasible to implement.
Performance Security	Security should not cause excessive system performance degradation.

Funded by Horizon Europe Framework Programme of the European Union

Cybersecurity Principles	Description
Human-Factored Security	Security controls should be designed with human behaviour in mind.
Acceptable Security	Security controls should align with business needs and operational priorities.
Latent Design Conditions	Unintended security risks emerge due to past design decisions and evolving system complexity.
Precautionary Principle	Proactively consider security and privacy implications before large-scale deployment.
Reference Monitor Concept	Defines an abstract security control to enforce system-wide policies.
Defence in Depth	Uses multiple layers of security controls to minimize risk.
Isolation	Separates critical components physically or logically to prevent unauthorized access.

Table 6 Cybersecurity principles from ISO 27701

Privacy Principles	Description
User Rights and Empowerment	
Consent of Choice	User must agree to data use willingly and clearly. Options to accept or deny must be easy to find and use
Individual Participation and Access	Users should be able to access and manage their data easily.
Accuracy and Quality	Data must be correct and up-to-date. Must allow users to fix mistakes in their data
Purpose and Data Limitation	
Purpose Legitimacy and Specification	Data must only be collected for clear, legal purposes. Users should know exactly why their data is being collected
Collection Limitation	Only collect minimum data needed for the purpose
Data Minimization	collecting, processing, and retaining only the minimum amount of data necessary to fulfil a specific purpose

Funded by Horizon Europe Framework Programme of the European Union

Privacy Principles	Description
Use, Retention and Disclosure Limitation	personal data is collected, used, and retained only for specific, explicit, and legitimate purposes
Transparency and Accountability	
Openness, Transparency and Notice	Clearly explain what data is collected, why, and how it's used. Make privacy policies easy to find and understand.
Accountability	Organizations must prove they follow privacy rules. Keep privacy practices well-documented.
Privacy Compliance	Regularly monitor, evaluate and ensure compliance with applicable privacy regulations and standards
Data Security and Protection	
Information Security	Protect data with strong safeguards (e.g., encryption, access control)

Table 7 Data Quality Characteristics from ISO/IEC 25012 :2008 – Data Quality Model [19]

Data Quality Principles	Description
Inherent Data Quality Dimensions	
Accuracy	The degree to which data has attributes that correctly represent the true value of the intended attribute of a concept or event in a specific context of use. It has two main aspects: • Syntactic Accuracy: Syntactic accuracy is defined as the closeness of the data values to a set of values defined in a domain considered syntactically correct. • Semantic Accuracy: Semantic accuracy is defined as the closeness of the data values to a set of values defined in a domain considered semantically correct.
Completeness	The degree to which subject data associated with an entity has values for all expected attributes and related entity instances in a specific context of use.
Consistency	The degree to which data has attributes that are free from contradiction and are coherent with other data in a specific context of use. It can be either or both among data regarding one entity and across similar data for comparable entities.

Funded by Horizon Europe Framework Programme of the European Union

Data Quality Principles	Description
Credibility	The degree to which data has attributes that are regarded as true and believable by users in a specific context of use. Credibility includes the concept of authenticity (the truthfulness of origins, attributions, commitments).
Currentness	The degree to which data has attributes that are of the right age in a specific context of use.
Inherent and System-Dependent Data Quality Dimensions	
Accessibility	The degree to which data can be accessed in a specific context of use, particularly by people who need supporting technology or special configuration because of some disability.
Compliance	The degree to which data has attributes that adhere to standards, conventions or regulations in force and similar rules relating to data quality in a specific context of use.
Confidentiality	The degree to which data has attributes that ensure that it is only accessible and interpretable by authorized users in a specific context of use. Confidentiality is an aspect of information security.
Efficiency	The degree to which data has attributes that can be processed and provide the expected levels of performance by using the appropriate amounts and types of resources in a specific context of use.
Precision	The degree to which data has attributes that are exact or that provide discrimination in a specific context of use.
Traceability	The degree to which data has attributes that provide an audit trail of access to the data and of any changes made to the data in a specific context of use.
Understandability	The degree to which data has attributes that enable it to be read and interpreted by users, and are expressed in appropriate languages, symbols and units in a specific context of use. Some information about data understandability are provided by metadata.
System-Dependent Data Quality Dimensions	
Availability	The degree to which data has attributes that enable it to be retrieved by authorized users and/or applications in a specific context of use.

Funded by Horizon Europe Framework Programme of the European Union

Data Quality Principles	Description
Portability	The degree to which data has attributes that enable it to be installed, replaced or moved from one system to another preserving the existing quality in a specific context of use.
Recoverability	The degree to which data has attributes that enable it to maintain and preserve a specified level of operations and quality, even in the event of failure, in a specific context of use.

4.2.2 Workflow

The risk management framework workflow follows a shared responsibility model between the manufacturer of the CMD, the Hospitals and the patients, as shown in Figure 11.

According to the Cylcomed Risk Management Framework, the Manufacturers' role in this framework is the following. First, a structured modelling of the CMD must be performed. This is done recurring to the Data Flow Diagrams framework, outline previously. Then, the manufacturer uses the Cyber-Kill Chain methodology to determine the threats and countermeasures it must apply to the CMD. The manufacturer should consider the environment of operation of the CMD (e.g., home, hospital, ambulance) when doing the threat modelling. Then, these cybersecurity threats, which can enable hazardous situations should be matched with the respective benefits they will impact. A qualitative MCDA analysis is performed in order to understand if the CMD is considered safe for use. Afterwards, the manufacturer should determine which are the most effective cybersecurity countermeasures, building upon the performed threat modelling. These countermeasures are going to impact the CMD functioning. These impact factors should be matched to the respective hazardous situations and the benefits of the device. Afterwards, a qualitative MCDA analysis is performed again.
The Healthcare Providers' role is to guarantee the overall safety of patients, and the cybersecurity of the hospitals' infrastructure. The hospitals already has to have their own cybersecurity risk management system in place and the process can be described in a simplified manner, which can be seen as similar to that of the manufacturer. Healthcare providers should perform an infrastructure analysis using frameworks like the Structured Modelling with Data Flow Diagrams. Then, they should perform a threat modelling process, followed by a benefit-risk evaluation process and then the selection of cybersecurity controls.

The user, or patient, will be instructed by the CMD manufacturers (e.g., via user guides and best practices), as well as the healthcare providers when introducing the device to the patient.

The framework predicts feedback loops between the CMD manufacturers, the Healthcare providers and the patient to enable the update of risks, benefits and cybersecurity controls to further improve the overall cybersecurity.

Funded by Horizon Europe Framework Programme of the European Union

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

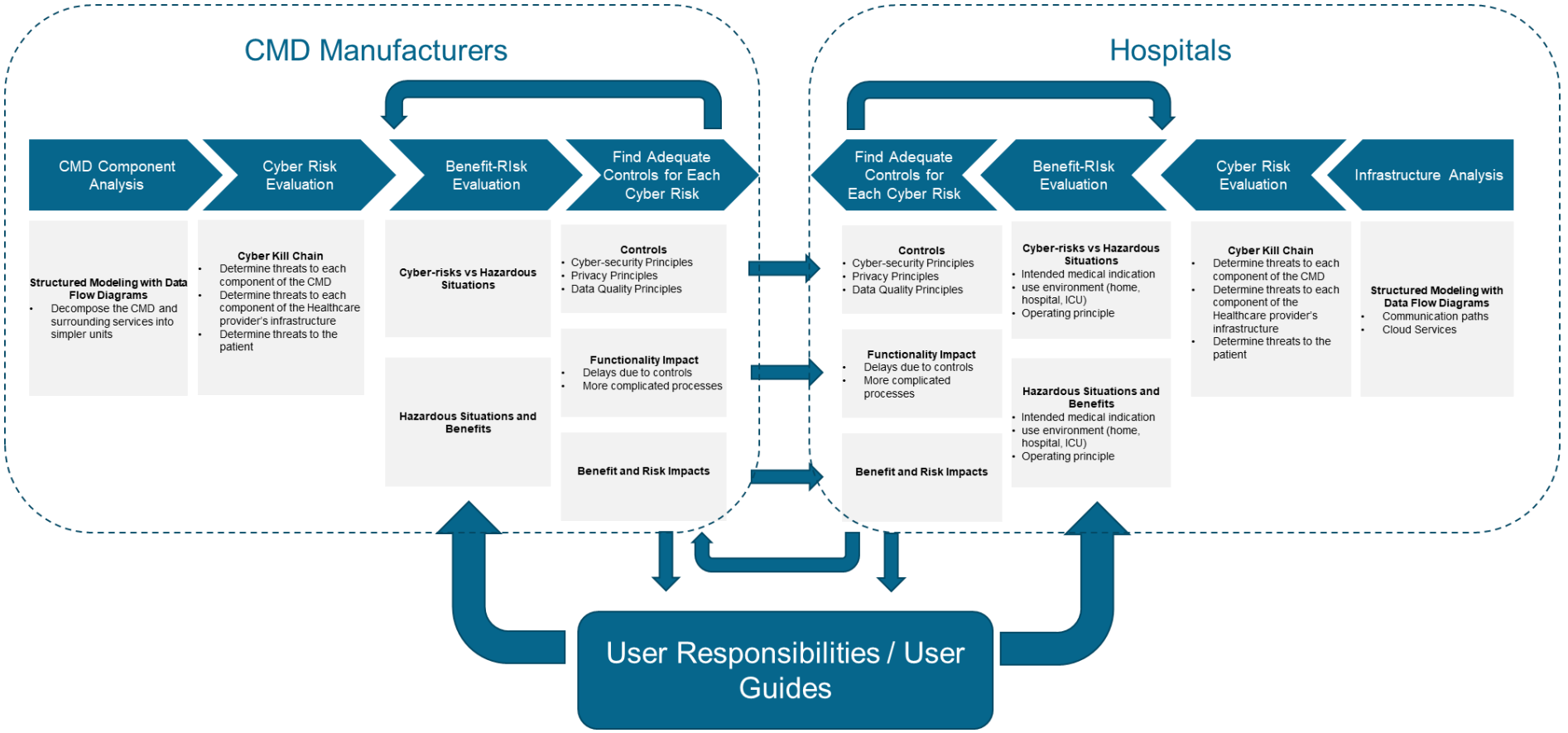

Figure 11 CYLCOMED Risk Management Framework highlighting the shared responsibilities between manufacturers, hospitals and patients

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 12.

Figure 12 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`[2], which is used for JSON Web Token-based authentication and Role-Based Access Control and authorization.

[2] https://flask-praetorian.readthedocs.io/en/latest/

The frontend is powered by the React renderer and the styling is achieved using MUI Materials[3]. 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).

Data Model

The data model of the Risk Management Tool is shown in Figure 13.

[3] *https://mui.com/*

Funded by Horizon Europe Framework Programme of the European Union

Figure 13 Risk Management Tool – data model

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 12:

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 analysis – process of attributing a likelihood score and an impact score for the identified risks. The risk level is the resulting combination of the likelihood and the impact score, given by the risk matrix.
6. Risk evaluation – The process of selecting, for each risk, what the action to be taken: avoid the risk, accept the risk, mitigate the risk and transfer the risk.
7. 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. This is needed whenever the risk mitigation action is selected during the risk evaluation phase.
8. 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 materializes.

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 final version 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.

Authorizations and corresponding frontend pages

Authorization is based on Role-based Access Control (RBAC). Each user has an associated role, which is reflected on the actions they can perform on the tool.

The Risk Management Tool opening page is presented in Figure 14.

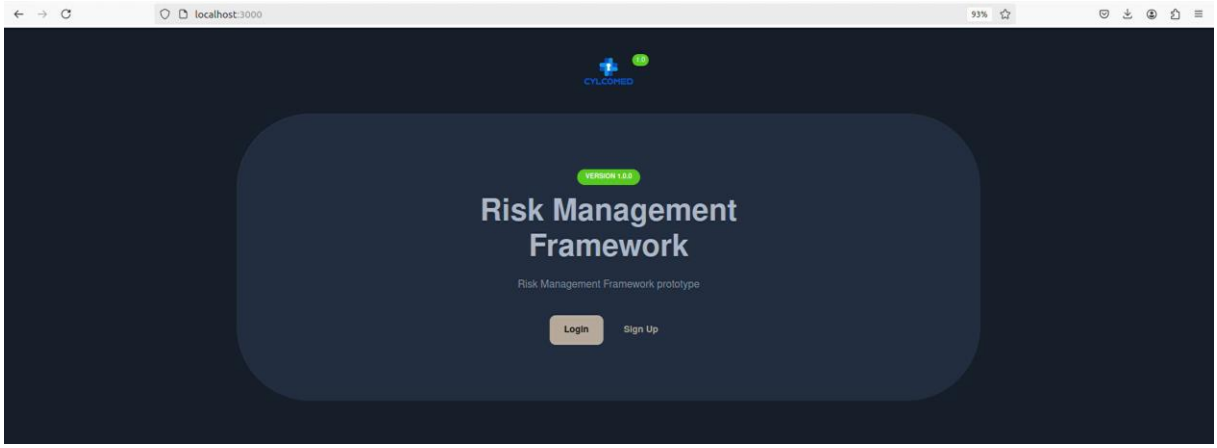

Figure 14 Risk Management Tool – homepage

Every user must perform the sign up before the role is assigned to them (please refer to Figure 15 for the sign-up page). The first user to sign up will be automatically the user manager.

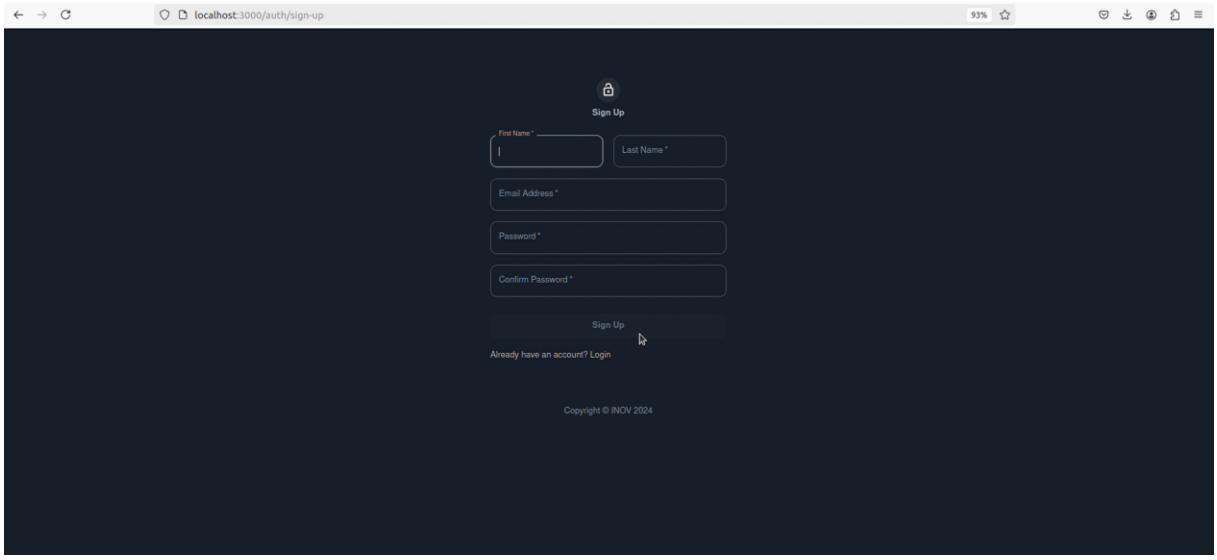

Figure 15 Risk Management Tool – sign up page

The User Manager is the role that grants permissions to an account to manage the user-base, including the attribution of roles, or the deletion of accounts. The user manager dashboard is depicted in Figure 16.

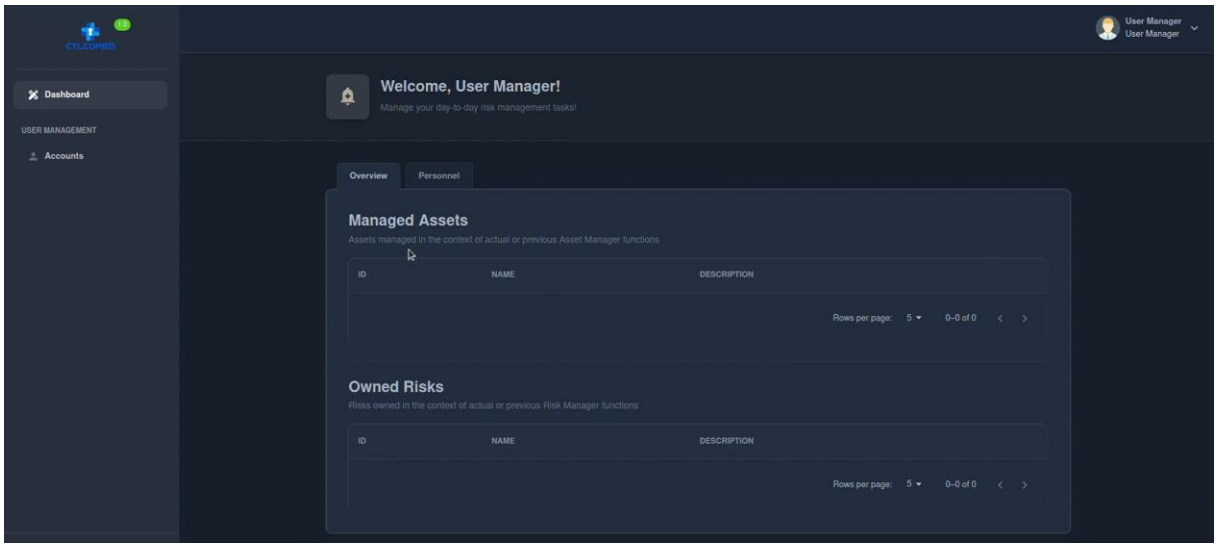

Figure 16 User manager Dashboard

In Figure 17 the user manager views the pending role accounts. Pending role 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. The user manager selects the adequate role to the account in Figure 18 and Figure 19.

Funded by Horizon Europe Framework Programme of the European Union

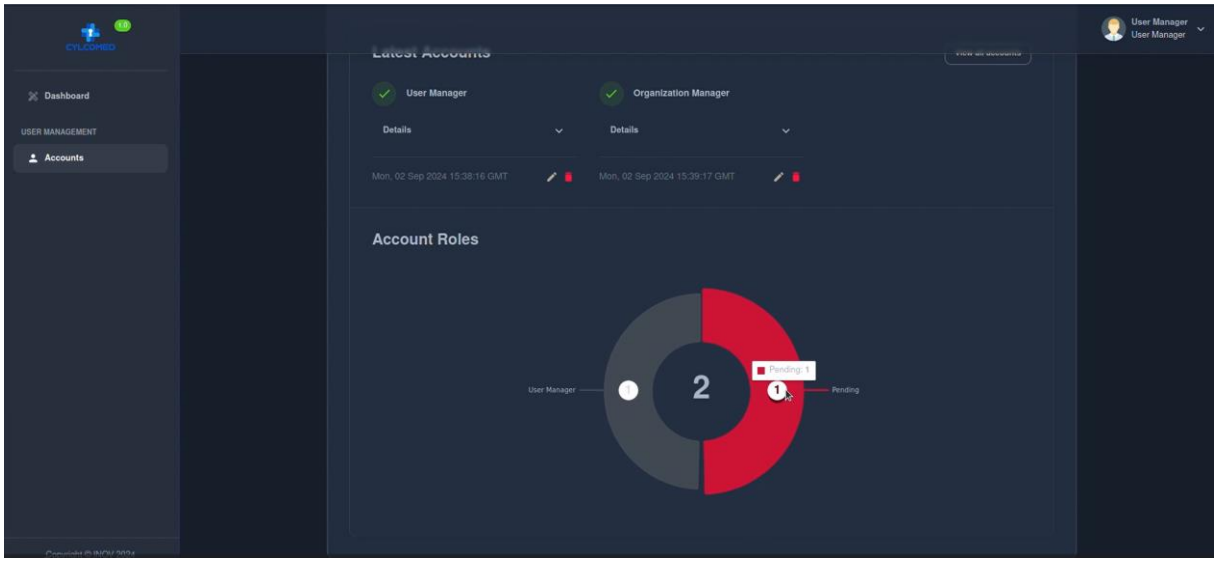

Figure 17 User manager viewing pending roles

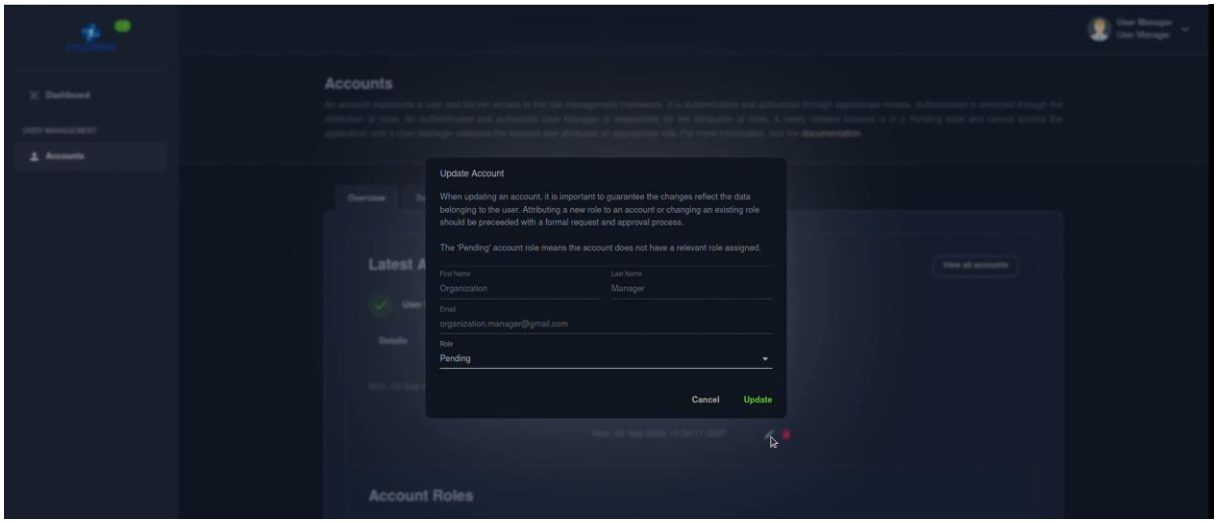

Figure 18 User manager selecting a pending role account

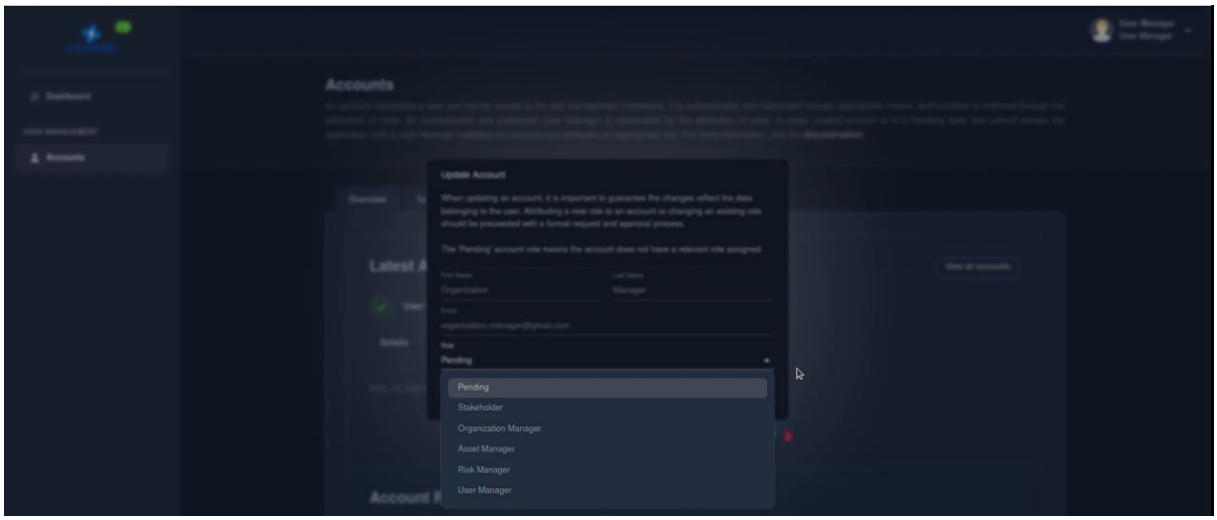

Figure 19 User manager assigning a role to a pending account

Funded by Horizon Europe Framework Programme of the European Union

The Organization Manager is the role responsible for adding the standards (Figure 20) and cybersecurity controls (Figure 21) to be applied to assets. In Figure 22 the organization manager is viewing the controls he introduced.

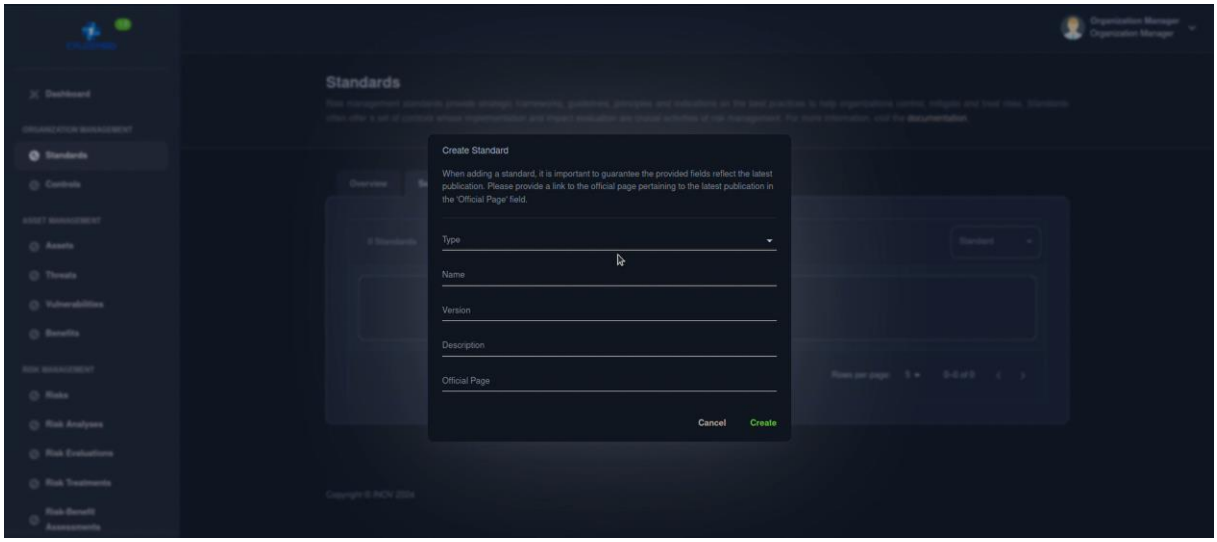

Figure 20 Organization manager creating a standard

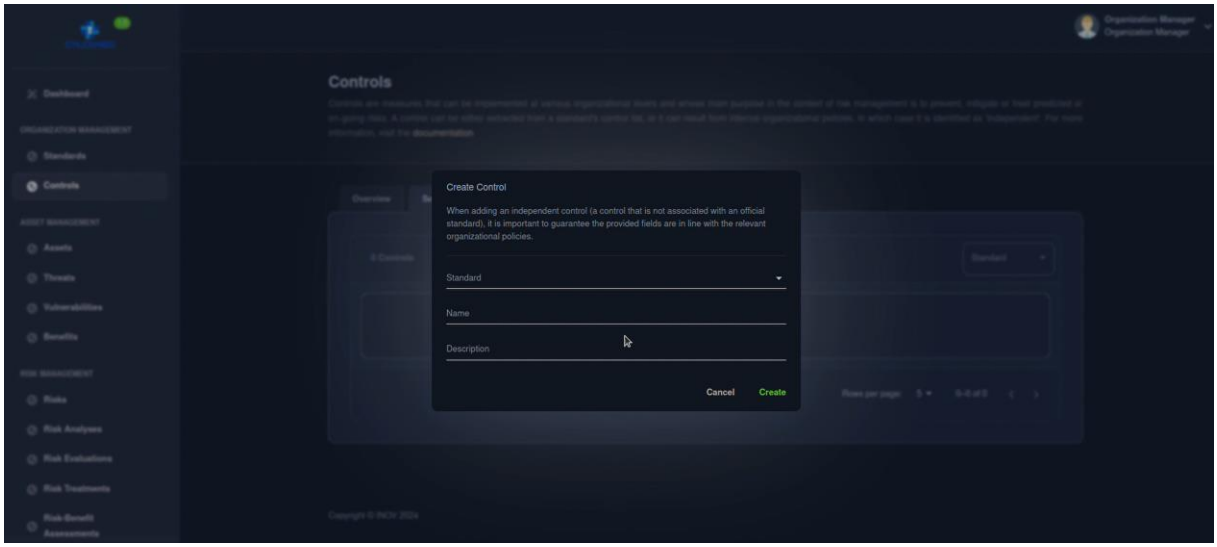

Figure 21 Organization manager creating cybersecurity controls

Funded by Horizon Europe Framework Programme of the European Union

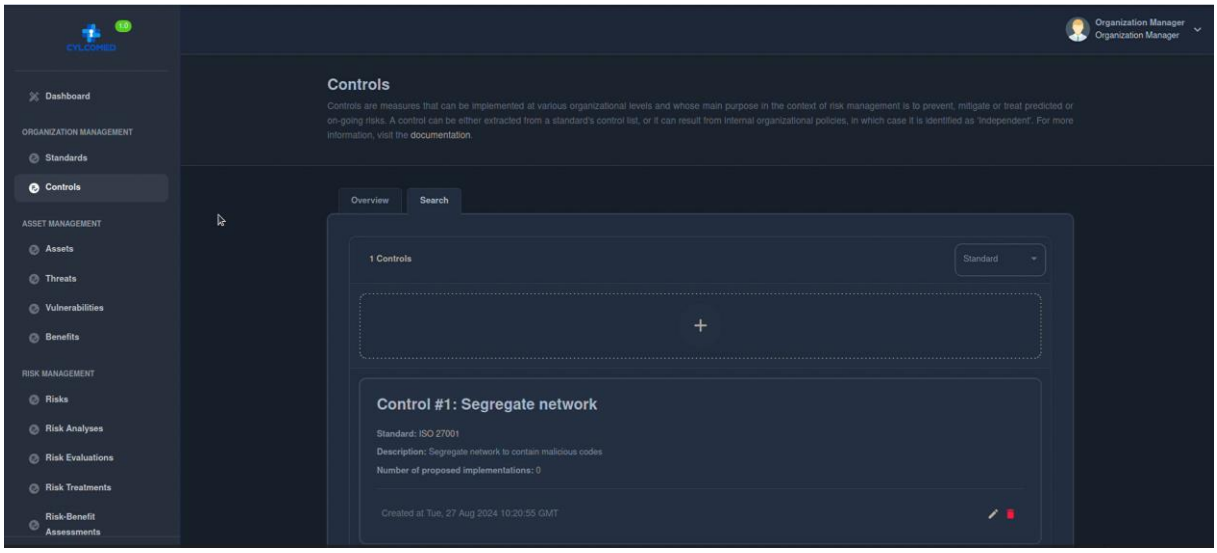

Figure 22 Organization Manager viewing created controls

The Asset Manager role responsible for creating assets (Figure 23), creating vulnerabilities (Figure 25), creating threats (Figure 24) and creating benefits (Figure 26).

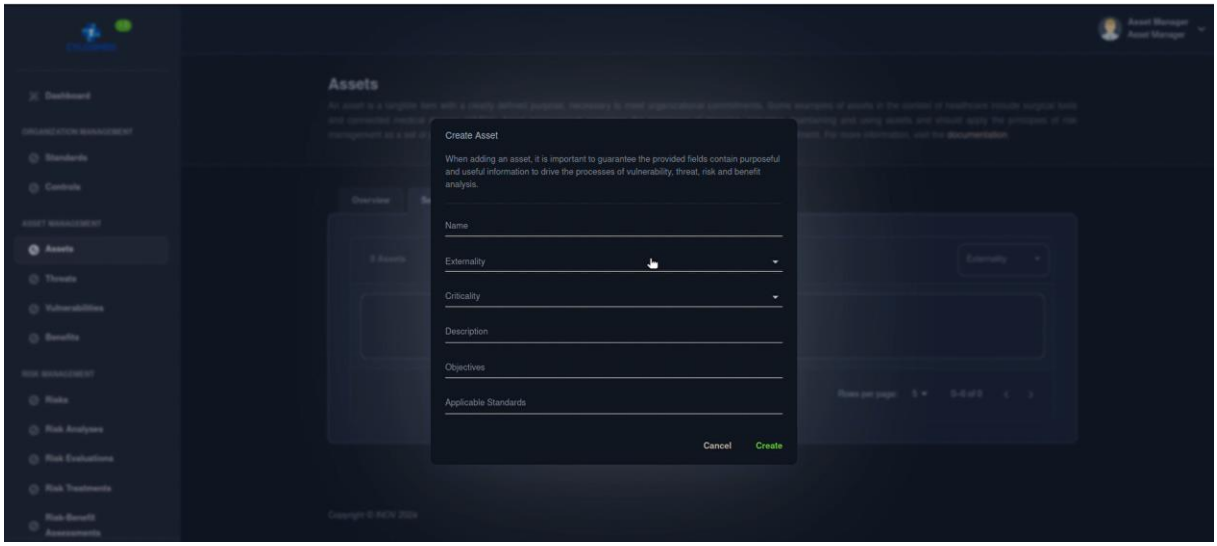

Figure 23 Asset manager creating assets (e.g., CMD)

Funded by Horizon Europe Framework Programme of the European Union

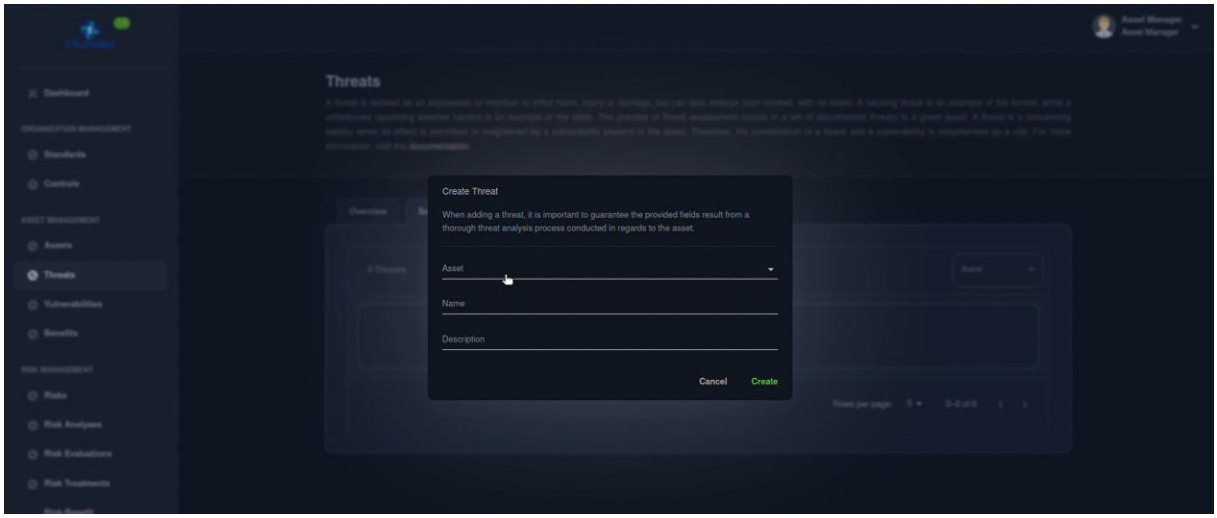

Figure 24 Asset Manager creating threat associated to an asset

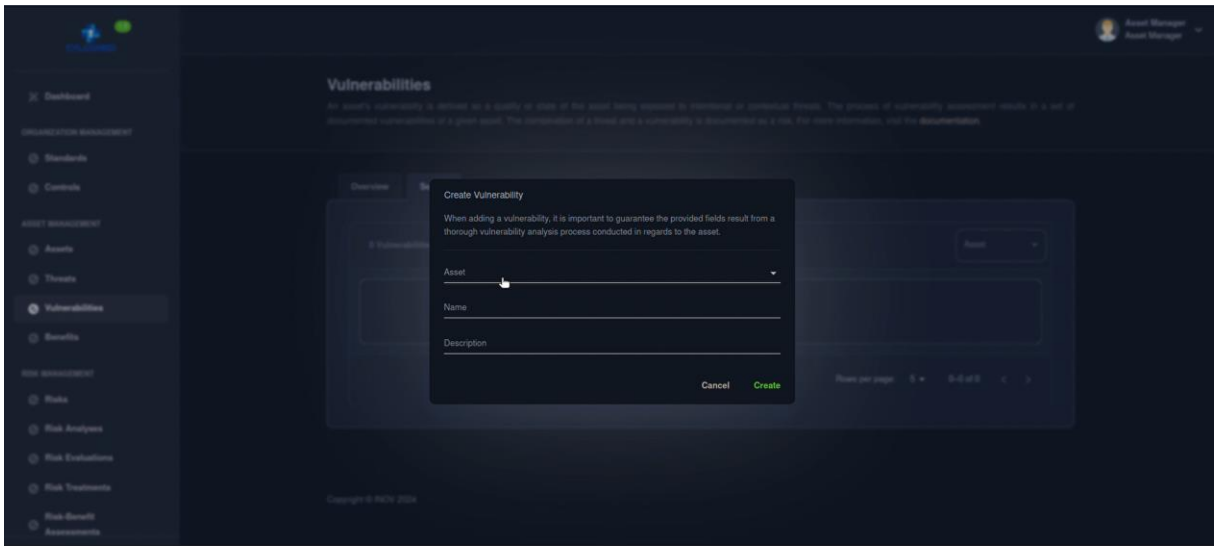

Figure 25 Asset Manager creating a vulnerability for an asset

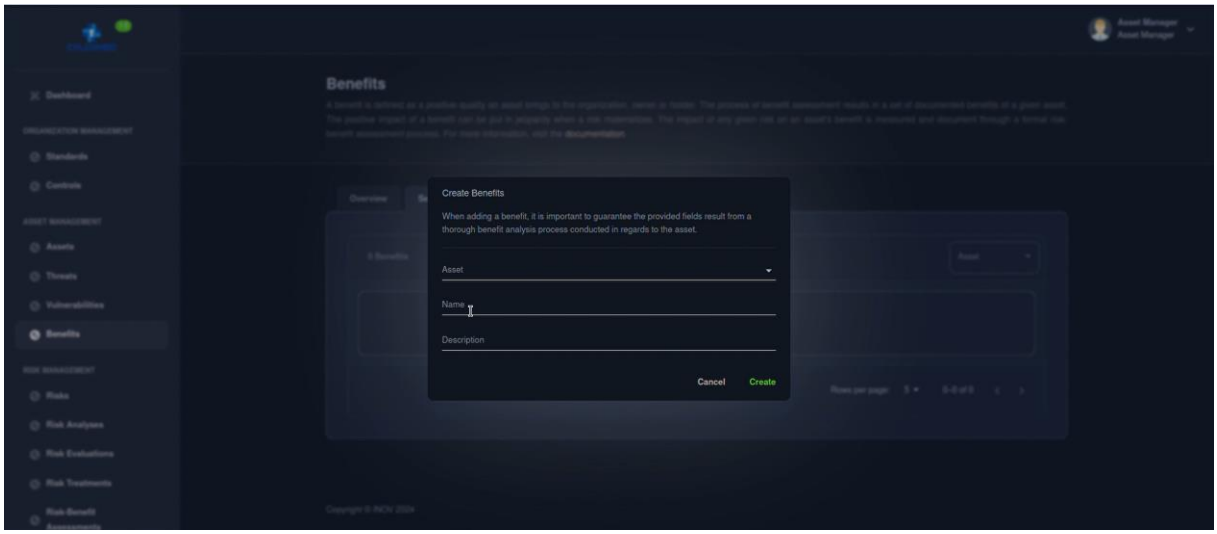

Figure 26 Asset Manager creating a benefit for an asset

Funded by Horizon Europe Framework Programme of the European Union

Risk Manager is the role responsible for creating the risks (Figure 27), performing risk analysis (Figure 28, Figure 29), risk evaluation (Figure 30), risk benefit analysis (Figure 33, Figure 34) and risk treatment selection (Figure 31, Figure 32).

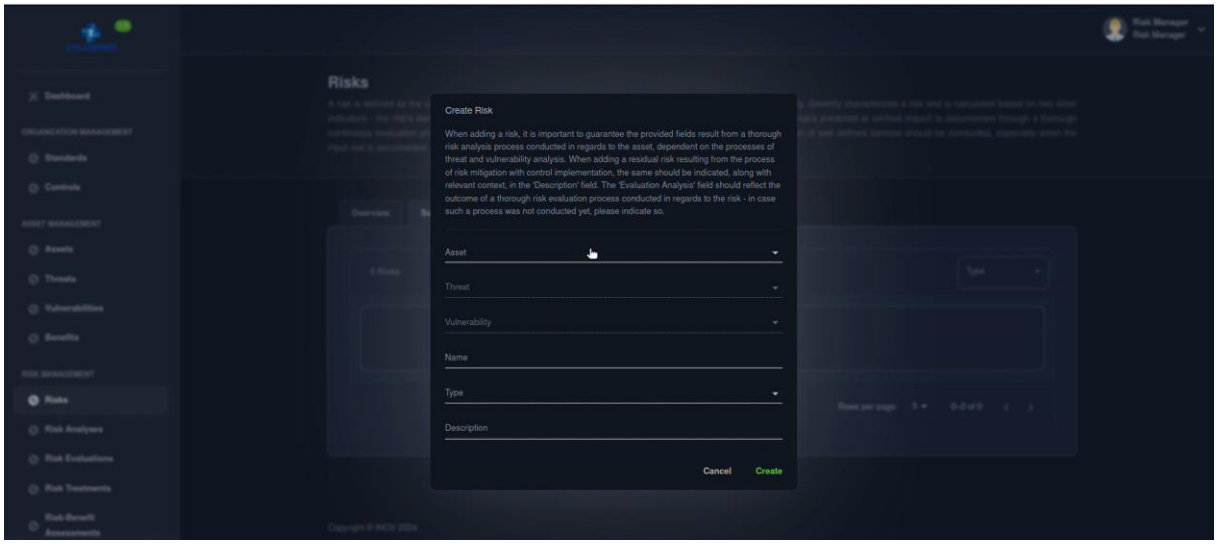

Figure 27 Risk Manager creating a risk, selecting an asset, a threat and respective vulnerability that was introduced formerly by the asset manager

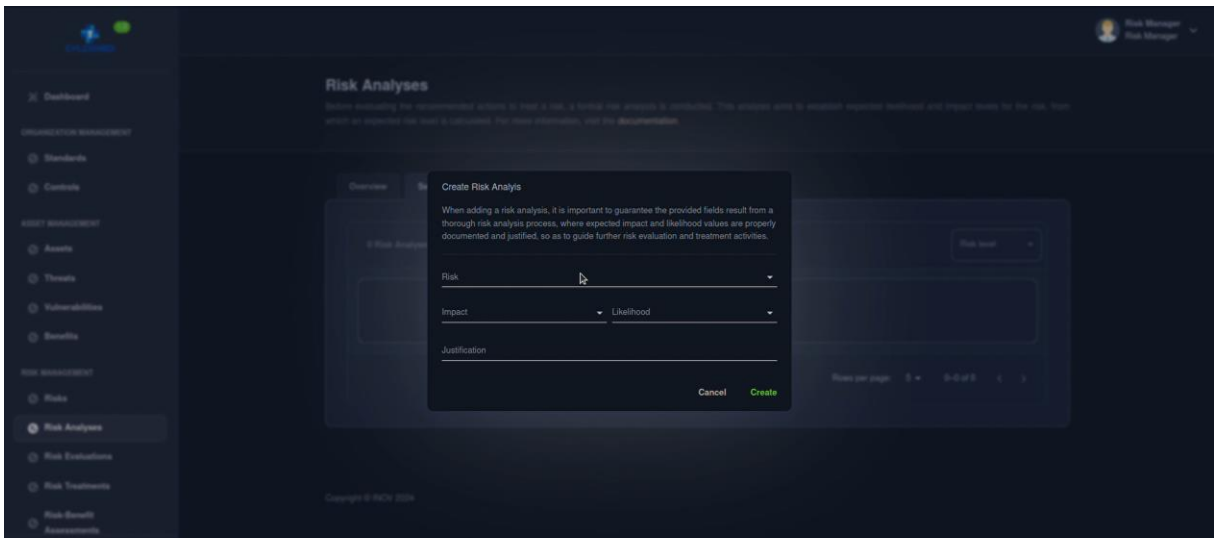

Figure 28 Risk Manager performing risk analysis, selecting the risk and respective impact and likelihood.

Funded by Horizon Europe Framework Programme of the European Union

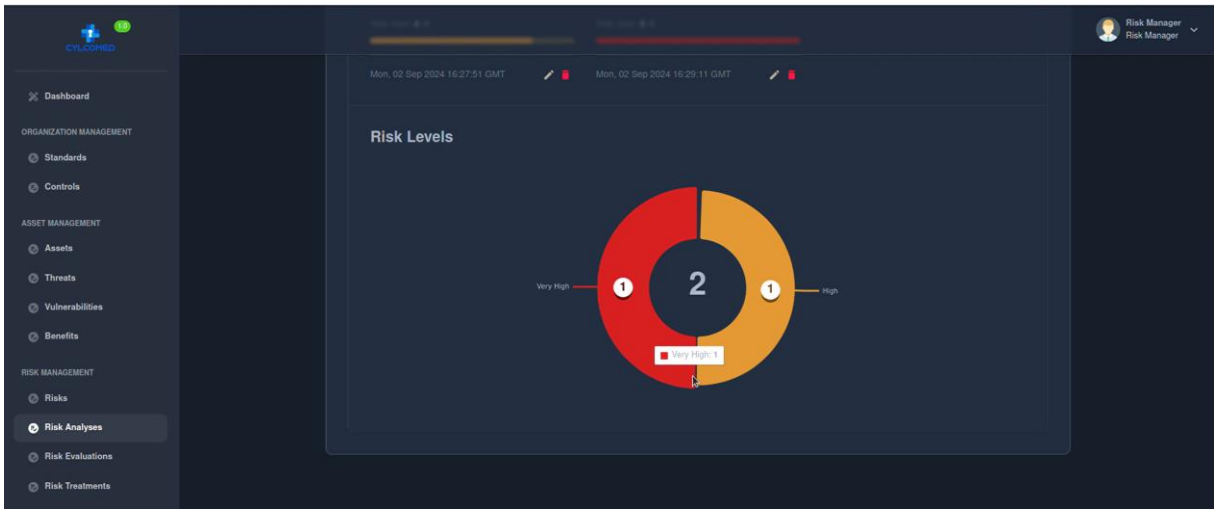

Figure 29 Risk Manager in the risk analyses view, showing the number of risks in each of the risk levels

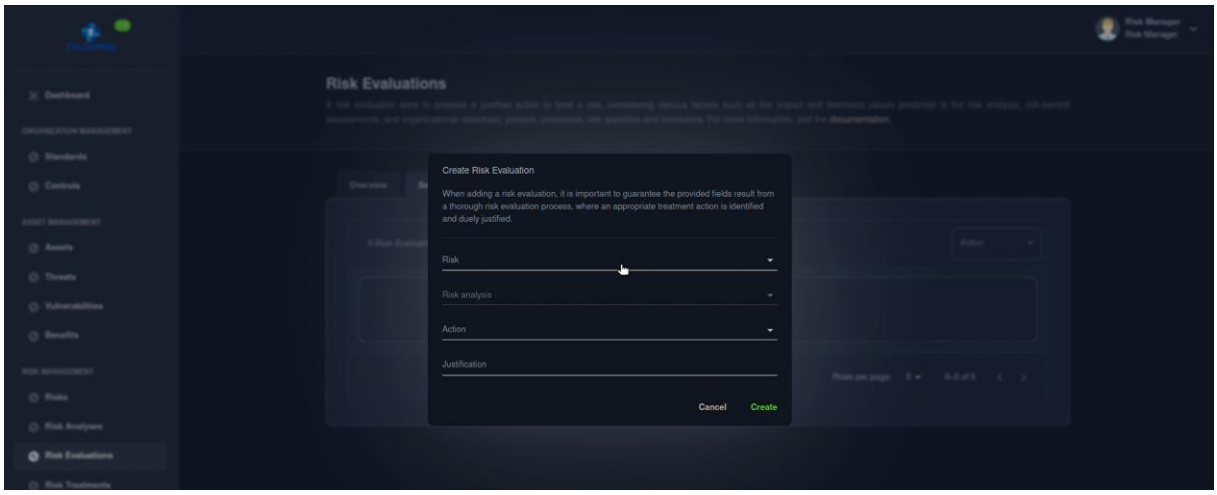

Figure 30 Risk Manager creating the risk evaluation – selecting for a risk, the action to be taken

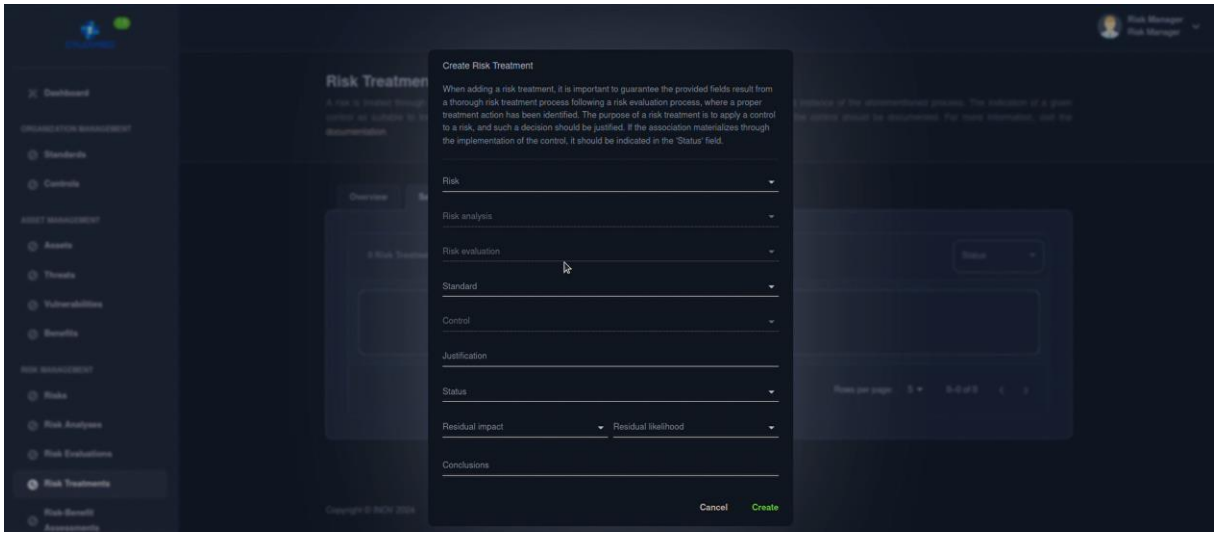

Figure 31 Risk manager creating risk treatment

Funded by Horizon Europe Framework Programme of the European Union

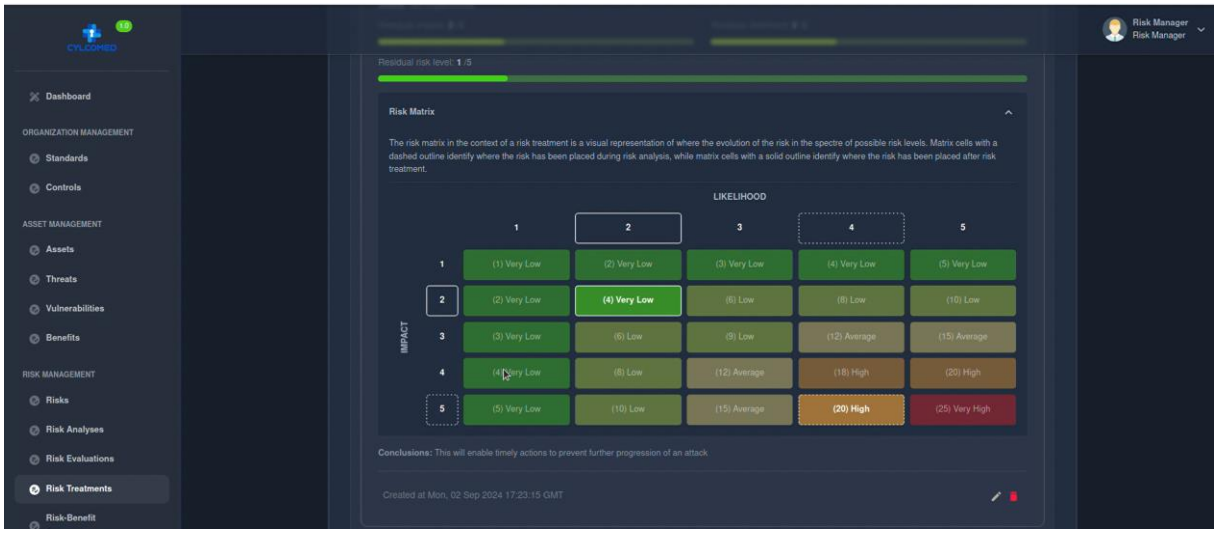

Figure 32 Risk manager in the risk treatment view, viewing a risk level after a risk treatment is implemented, reducing it from High (20) to very low (4).

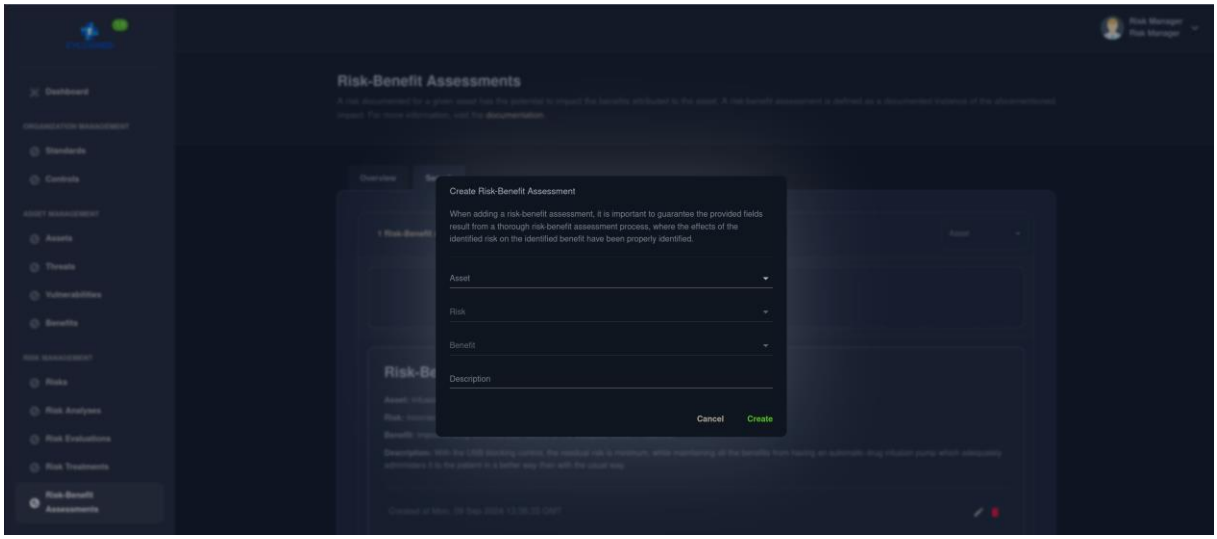

Figure 33 Risk manager performing the risk-benefit assessment.

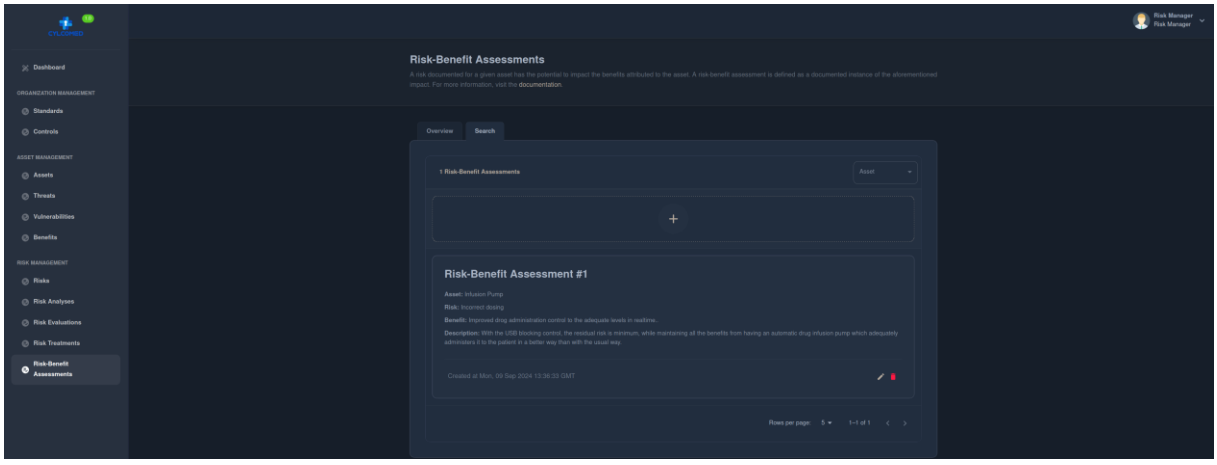

Figure 34 Risk manager in the risk-benefit assessment view.

There is one more role, the Stakeholder which can only read the risk management data, without being able to modify it.

Funded by Horizon Europe Framework Programme of the European Union

6 Conclusions

This deliverable documents the work done on the benefit-risk analysis scheme, the risk management framework and the risk management tool developed for the CYLCOMED project.

The benefit-risk scheme and the risk management framework was built on top of previously documented work on this project. The final version of the benefit-risk scheme resulted from the analysis of risk factors within the healthcare industry and risk factors within cybersecurity, which usually recurred to qualitative schemes with multi-criteria.

The Risk Management Framework, resulted from finding the common actions within the manufacturers risk management standard, the organizational cybersecurity risk management process, integrating the benefit-risk scheme developed in this project. It also included considerations from IoT, cloud, blockchain, AI and 5G documentation regarding cybersecurity and risk management.

Finally, the final software release of the Risk Management Tool was further developed having in mind a process-driven view, aligned with the risk management framework.

Regular feedback in critical decision points, during regular meetings and General Assembly meetings were important in the design and development of the benefit-risk scheme, the risk management framework and the Risk Management Tool.

The benefit-risk scheme, risk management framework and the Risk Management Tool will be tested in the Project's pilots.

Funded by Horizon Europe Framework Programme of the European Union

References

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

[2] F. A. Alzahrani, M. Ahmad and M. T. J. Ansari, "Towards Design and Development of Security Assessment Framework for Internet of Medical Things," *Applied Sciences,* vol. 12, no. 16, p. 8148, 2022.

[3] Portuguese National Cybersecurity Centre, “National Cybersecuity Framework,” Portuguese National Cybersecurity Centre, 2020.

[4] "Risk Analysis in Healthcare Organizations: Methodological Framework and Critical Variables," *[Journal Name],* vol. [Volume], no. [Issue], p. [Pages], [Year].

[5] . National Health Service (NHS), "Risk Register Report," National Health Service (NHS), 2022.

[6] "Risk Management Framework," NHS London Trust, 2022.

[7] U.S. Food and Drug Administration, “Factors to Consider Regarding Benefit-Risk in Medical Device Product Availability, Compliance, and Enforcement Decisions - Guidance for Industry and Food and Drug Administration Staff,” 2016.

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

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

[10] P. G. M. K. C. N. C. &. K.-R. P. Wahlster, “Balancing costs and benefits at different stages of medical innovation: A systematic review of Multi-Criteria Decision Analysis (MCDA),” *BMC Health Services Research,* vol. 15, no. 262, 2015.

[11] "Playbook for Threat Modeling Medical Devices," MITRE Corporation and Medical Device Innovation Consortium (MDIC), 2021.

[12] "How to Use Cyber Kill Chain Model to Build Cybersecurity," *Wroclaw Centre for Networking and Supercomputing,* pp. 1-XX, 2017.

[13] "Gaining the Advantage: Applying Cyber Kill Chain® Methodology to Network Defense," Lockheed Martin Corporation, 2015.

[14] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), “ISO/IEC 30141:2024 – Internet of Things (IoT) – Reference Architecture,” ISO/IEC, 2024.

Funded by Horizon Europe Framework Programme of the European Union

[15] H. A. a. M. A. T. Yaqoob, “Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review,” *IEEE Communications Surveys & Tutorials,* vol. 21, no. 4, pp. 3723-3768, 2019.

[16] [Online]. Available: https://homedialysis.org/home-dialysis-basics/machines-and-supplies/hemodialysis-machines#:~:text=HD%20machines%20clean%20blood%20by,the%20outside%20of%20the%20fibers.. [Accessed 11 March 2025].

[17] "Risk management for medical devices and the new BS EN ISO 14971," British Standards Institution, n.d..

[18] "Recognition of EN ISO 14971 as a Harmonized Standard in Support of the European Medical Device Regulations," ISO, n.d..

[19] [Online]. Available: https://iso25000.com/index.php/en/iso-25000-standards/iso-25012.

[20] S. Pericherla, “Cloud Computing Threats, Vulnerabilities and Countermeasures: A State-of-the-Art,” *International Journal of Information Security,* vol. 15, no. 1, pp. 1-58, January 2023.

[21] F. A. M. A. a. M. T. J. A. Alzahrani, “Towards Design and Development of Security Assessment Framework for Internet of Medical Things,” *Applied Sciences,* 2022.

[22] ENISA, “ENISA 5G Threat Landscape - Update,” 2022.

[23] ENISA, “ENISA Threat Landscape for 5G Networks - Threat assessment for the fifth generation of mobile telecommunications networks (5G),” 2019.

[24] ENISA, “5G Security Controls Matrix (version 1.3),” 2022. [Online]. Available: https://www.enisa.europa.eu/publications/5g-security-controls-matrix.

[25] ENISA, “Distributed Ledger Technology and Cybersecurity - Improving information security in the financial Sector,” 2016.

[26] NIST, “AI RMF Playbook,” 2024.

[27] F. A. Alzahrani, M. Ahmad and M. T. J. Ansari, “Towards Design and Development of Security Assessment Framework for Internet of Medical Things,” *Applied Sciences,* vol. 12, 2022.

[28] F. Antinious and S. Norimarna, “Risk Management Maturity Assessment based on ISO 31000 - A pathway toward the Organization's Resilience and Sustainability Post COVID-19: The Case Study of SOE Company in Indonesia,” in *3rd International Conference on Management, Economics and Finance*, Amsterdam, 2021.

[29] Institute of Risk Management, “A Risk Practitioners Guide to ISO 31000:2018,” Institute of Risk Management.

Funded by Horizon Europe Framework Programme of the European Union

[30] Australian Government Comcover, “An Overview of the Risk Management Process,” Australian Government Comcover.

Funded by Horizon Europe Framework Programme of the European Union

Appendix A. Cloud Cybersecurity

The lists of cloud vulnerabilities, risks and countermeasures were derived from [20].

Table 8 Vulnerabilties of Cloud technology, extracted from [20]

Vulnerability Name	Service Model(s) Susceptible to Vulnerabilities	Description
Vulnerable Systems and APIs	SAAS, PAAS, IAAS	Vulnerabilities in operating systems, APIs, or other middleware might lead to the compromise of the subsystem or entire system.
Simple Human Errors	SAAS, PAAS, IAAS	Simple human errors such as misconfigurations or accidental deletions can lead to security breaches or data loss.
Application Vulnerabilities	SAAS, PAAS, IAAS	Applications may have security flaws that attackers can exploit to gain unauthorized access or compromise data.
Poor Security Policies	SAAS, PAAS, IAAS	Poorly defined or enforced security policies can leave cloud environments vulnerable to attacks.
Natural Disasters	IAAS	Natural disasters such as floods, earthquakes, or fires can physically damage data centres, leading to data loss.
Hard Drive Failures	IAAS	Hard drive failures can result in the loss of stored data, especially if there are no proper backups.
Power Failures	IAAS	Power failures can disrupt cloud services and cause temporary or permanent data loss.
Weak Authentication and Identity Management	SAAS, PAAS, IAAS	Malware infections can compromise cloud systems, leading to unauthorized access, data breaches, or service disruption.
Poor Credentials management practice	SAAS, PAAS, IAAS	A former employee with access credentials can misuse them to steal or tamper with data.
Poor System Administrator privilege management	SAAS, PAAS, IAAS	System administrators with privileged access can intentionally or unintentionally compromise security.
Third Party Contractor	SAAS, PAAS, IAAS	Third-party contractors with access to cloud systems may pose security risks if not properly vetted.
Weak Business Partner	SAAS, PAAS, IAAS	Weak security measures among business partners can expose an organization’s cloud resources to threats.
Weak Network Architecture	SAAS, PAAS, IAAS	A poorly designed network architecture can make cloud environments vulnerable to attacks such as DDoS.
Insecure Network Protocol	SAAS, PAAS, IAAS	Insecure network protocols can expose data transmissions to eavesdropping or interception by attackers.

Funded by Horizon Europe Framework Programme of the European Union

Vulnerability Name	Service Model(s) Susceptible to Vulnerabilities	Description
Vulnerable Application	SAAS, PAAS, IAAS	Applications with known vulnerabilities can be exploited by attackers to gain unauthorized access.
Weak API Credentials	SAAS, PAAS, IAAS	Weak API credentials, such as default passwords, can be exploited by attackers to gain control over cloud resources.
Poor Key Management	SAAS, PAAS, IAAS	Poor key management practices can lead to unauthorized access and data breaches.
Operating System Bugs	SAAS, PAAS, IAAS	Bugs in operating systems used in cloud environments can introduce security vulnerabilities.
Hypervisor Bugs	SAAS, PAAS, IAAS	Hypervisor bugs can allow attackers to escape virtual machines and access other users' data.
Unpatched Software	SAAS, PAAS, IAAS	Unpatched software can leave cloud environments vulnerable to known exploits.
Users' Lack of Awareness	SAAS, PAAS, IAAS	Social engineering attacks trick users into divulging sensitive information, such as login credentials.
Shared Technology Vulnerabilities	SAAS, PAAS, IAAS	As the cloud provides multi-tenancy, vulnerabilities in virtual machines and hypervisors might allow attackers to compromise all users sharing the resources.
VM Vulnerabilities	PAAS, IAAS	Vulnerabilities in virtual machines can be exploited to compromise cloud security.
Third-Party Software Vulnerabilities	PAAS, IAAS	Third-party software used in the cloud may introduce security risks if it contains vulnerabilities.
No Auditing	SAAS	A lack of auditing can prevent organizations from detecting and mitigating security threats.
Service Level Agreement Issues	SAAS	Issues with service level agreements (SLAs) can lead to misunderstandings regarding security responsibilities.
Lacking Due Diligence	SAAS, PAAS, IAAS	A cloud consumer must periodically review the accreditations and standards followed by the cloud service provider.
Lack of USB port protection / policies	SAAS, PAAS, IAAS	Malware introduced via USB devices can infect cloud-connected systems.
Inse3cure Third-Party APIs	SAAS, PAAS, IAAS	Insecure third-party APIs can expose cloud environments to security risks.
No Cloud Service Monitoring	PAAS, IAAS	A lack of continuous monitoring in cloud services can allow security breaches to go undetected.
Human Negligence	SAAS, IAAS	Negligence by human operators can lead to security breaches or data loss.
None or Insufficient Security Training	SAAS, IAAS	Insufficient security training can result in employees being unaware of security best practices.

Funded by Horizon Europe Framework Programme of the European Union

Vulnerability Name	Service Model(s) Susceptible to Vulnerabilities	Description
Infrastructure Vulnerabilities	SAAS, IAAS	Infrastructure vulnerabilities can make cloud environments susceptible to security threats.
Platform Vulnerabilities	SAAS, IAAS	Platform vulnerabilities can be exploited to gain unauthorized access or disrupt cloud services.
Hardware Design Vulnerabilities	IAAS	Hardware design flaws can introduce security weaknesses in cloud environments.
Weak Device Management	SAAS, IAAS	Weak device management practices can allow attackers to exploit IoT or other cloud-connected devices.
Unprotected IoT Devices	IAAS, PAAS, SAAS	A misconfigured device might allow a perpetrator to access other devices in the network and thereby cause damage to the system by accessing sensitive information.

Table 9 Threats of Cloud technology, extracted from [20]

Threat Name	Description
Data Breaches	A data breach is the disclosure of sensitive information to unauthorized parties either intentionally or unintentionally.
Data Loss	Data loss is the unavailability of data due to software or hardware failure, natural disasters, or human errors.
Malicious Insiders	A former employee, system administrator, or business partner acting as a perpetrator in causing damage to the organization or business.
Denial of Service (DoS)	An attack in which a system or service is made inaccessible to legitimate users.
Targeted Attack	A targeted attack exploits specific vulnerabilities in a system to gain unauthorized access or cause damage.
Malware Infection	Malware infections can compromise cloud systems, leading to unauthorized access, data breaches, or service disruption.
Account Hijacking	Stolen credentials of cloud users or operators may allow illegitimate users to use cloud resources for nefarious purposes.
Man-In-The-Middle (MITM) Attack	Man-in-the-middle attacks intercept communication between users and cloud services, leading to data theft.
Direct Hacking	Direct hacking involves exploiting security weaknesses to gain unauthorized access to cloud services.
Advanced Persistent Threats (APT)	An attack in which the perpetrator infiltrates the system and continuously monitors it for sensitive information.
Abuse of Cloud Services	Weakly configured cloud facilities and services can be used by malicious users to launch attacks on co-resident users.
A Lack of Responsibility	Cloud users are responsible for securing their application workloads in the cloud. Any negligence in doing so might lead to service unavailability or a data breach.
Insufficient Security Tools	Sophisticated attacks like DDoS cannot be mitigated to a full extent with the existing available open-source tools.

Funded by Horizon Europe Framework Programme of the European Union

Threat Name	Description
Human Error	The weakest link in security is the human element. A simple mistake by a system administrator might wreak havoc in the system.
Ransomware	A type of malware that compromises the availability of the system or service by encrypting the data and thereby making it unusable.
Spectre and Meltdown	Hardware-level vulnerabilities that allow attackers to access co-resident users' data or even compromise the hypervisor.
Network Penetration	Attackers may attempt network penetration to gain unauthorized access to cloud environments.

Table 10 Countermeasures for Cloud technology, extracted from [20]

Countermeasure Name	Description
Cryptography	Utilizing encryption techniques such as AES, Homomorphic Encryption, and Attribute-Based Encryption to secure data at rest and in transit.
Intrusion Detection Systems (IDS)	Implementing Host-based (HIDS) and Network-based (NIDS) intrusion detection systems to monitor and prevent unauthorized access.
Secure Authentication Mechanisms	Using Public Key Infrastructure (PKI), Single Sign-On (SSO), and Lightweight Directory Access Protocol (LDAP) to strengthen authentication.
Access Control Policies	Enforcing strict access control mechanisms to prevent unauthorized access and mitigate insider threats.
Virtual Firewalls	Deploying virtual firewalls to filter traffic and prevent malicious network intrusions in cloud environments.
Anomaly Detection Frameworks	Developing machine learning-based anomaly detection frameworks to identify and respond to unusual activities in cloud services.
Secure APIs	Ensuring that APIs use strong authentication, encryption, and regular security audits to mitigate vulnerabilities.
Data Backup and Disaster Recovery	Implementing regular data backup procedures and disaster recovery plans to prevent data loss due to failures or cyberattacks.
Service Level Agreements (SLA) Compliance	Ensuring cloud providers adhere to security and compliance standards defined in SLAs to protect users from breaches and service failures.
User Security Training	Educating employees and users about security best practices to reduce human error and social engineering attacks.
Monitoring and Logging	Enabling continuous monitoring and logging of cloud activities to detect and respond to potential threats effectively.
Secure Hypervisor Management	Ensuring that hypervisors are patched, configured securely, and protected against vulnerabilities to prevent VM escapes.

Funded by Horizon Europe Framework Programme of the European Union

Countermeasure Name	Description
Multi-Factor Authentication (MFA)	Requiring multi-factor authentication to strengthen login security and prevent account hijacking.
Blockchain for Security	Leveraging blockchain technology for secure identity management, access control, and data integrity verification.
Security Information and Event Management (SIEM)	Implementing SIEM systems to aggregate, analyze, and respond to security threats in real-time.
Threat Intelligence and Security Audits	Regularly conducting security audits and utilizing threat intelligence to proactively address potential vulnerabilities.
Zero Trust Architecture	Adopting a Zero Trust model to enforce strict verification of every request to prevent unauthorized access.

Funded by Horizon Europe Framework Programme of the European Union

Appendix B. IoT Cybersecurity

The lists of vulnerabilities, threats and countermeasures were extracted from [21].

Table 11 Vulnerabilties of IoT technology, extracted from [21]

Vulnerability	Description
Software vulnerabilities	The likelihood of software vulnerabilities has increased as a result of the large number of software applications in medical equipment.
Device Misuse	Threats posed by insiders who have authorized access but misuse it to compromise system security.
Improper physical access control	Deliberate attacks such as theft, vandalism, or sabotage to medical equipment.
Wireless vulnerabilities	Wireless threats such as jamming, eavesdropping, replay, and injection attacks that compromise medical devices.
Insecure protocols	Medical devices use open TCP/UDP docks and enable protocols such as TFTP, FTP, and Telnet, which are susceptible to attacks by default.
Weak authentication methods	Inadequate authentication mechanisms, such as the use of default credentials or weak password storage.
Weak Firmware Update Process	Lack of verification in firmware update mechanisms, making devices vulnerable to unauthorized modifications.
Data integrity risks Outdated Systems	Modification of patient data during processing, which can impact patient safety and treatment decisions. Medical tools are very seldom modified or retired from service. Remote cyberattacks can exploit these outdated systems.

Table 12 Threats of IoT technology, extracted from [21]

Threat	Description
Malware	Software programs designed to carry out unwanted and unauthorized actions on a system without the consent of the user, resulting in damage, corruption, or information theft. Its impact can be high.
Ransomware	Malicious software that encrypts critical healthcare data and demands a ransom for its release.
Crypto-jacking threats	Vulnerable medical devices being exploited for cryptocurrency mining, affecting their performance and longevity.
Exploit Kits	Code designed to take advantage of a vulnerability in order to gain access to a system. This threat is difficult to detect and in IoT environments its impact ranges from high to crucial, depending on the assets affected.

Funded by Horizon Europe Framework Programme of the European Union

Threat	Description
Targeted Attacks	Attacks designed for a specific target, launched over a long period of time, and carried out in multiple stages. The main objective is to remain hidden and to obtain as much sensitive data/information or control as possible. While the impact of this threat is medium, detecting them is usually very difficult and takes a long time.
DDoS	Multiple systems attack a single target in order to saturate it and make it crash. This can be done by making many connections, flooding a communication channel, or replaying the same communications over and over.
Counterfeit by Malicious Devices	This threat is difficult to discover, since a counterfeit device cannot be easily distinguished from the original. These devices usually have backdoors and can be used to conduct attacks on other ICT systems in the environment.
Physical attacks by unauthorized individuals	Threats posed by outsiders who gain unauthorized physical access to medical devices.
Attacks on Privacy	This threat affects both the privacy of the user and the exposure of network elements to unauthorized personnel.
Modification of Information	In this case, the objective is not to damage the devices, but to manipulate the information in order to cause chaos, or acquire monetary gains.
Man in the Middle	Active eavesdropping attack, in which the attacker relays messages from one victim to another, in order to make them believe that they are talking directly to each other.
IoT Communication Protocol Hijacking	Taking control of an existing communication session between two elements of the network. The intruder is able to sniff sensitive information, including passwords. The hijacking can use aggressive techniques like forcing disconnection or denial of service.
Wireless-based attacks	Wireless threats such as jamming, eavesdropping, replay, and injection attacks that compromise medical devices.
Interception of Information	Unauthorized interception (and sometimes modification) of a private communication, such as phone calls, instant messages, e-mail communications.

Funded by Horizon Europe Framework Programme of the European Union

Table 13 Countermeasures of IoT technology, extracted from [21]

Countermeasure	Description
Sign code cryptographically	Ensure the code has not been tampered with after being signed as safe for the device, and implement run-time protection and secure execution monitoring to ensure malicious attacks do not overwrite code after it is loaded.
Control software installation	Prevent unauthenticated software and files from being loaded onto operational systems.
Restore Secure State	Enable a system to return to a state that is known to be secure, after a security breach occurs or if an upgrade is not successful.
Enable security by default	Ensure that any applicable security features are enabled by default and that any unused or insecure functionalities are disabled by default.
Establish strong device passwords	Ensure that default passwords and even default usernames are changed during the initial setup, and that weak, null, or blank passwords are not allowed.
Limit permissions	Restrict the actions allowed for a given system by implementing fine-grained authorization mechanisms and applying the Principle of Least Privilege (POLP).
Use strong authentication	Require authentication mechanisms to use strong passwords or personal identification numbers (PINs), and consider using two-factor authentication (2FA) or multi-factor authentication (MFA) with methods such as smartphones, biometrics, or certificates.
Monitor device behaviour	Implement regular monitoring to verify the device behavior, detect malware, and discover integrity errors.
Establish asset management procedures	Maintain asset management procedures and configuration controls for key network and information systems.
Implement logging systems	Ensure that logging records events related to user authentication, account management, access rights, modifications to security rules, and system functionality.

Funded by Horizon Europe Framework Programme of the European Union

Appendix C. 5G Cybersecurity

The lists of vulnerabilities, threats and countermeasures were extracted from [22], [23], and [24] respectively.

Note that 5G technology has, not only the core and edge network cybersecurity concerns, but also IoT devices cybersecurity and cloud services cybersecurity to consider.

Table 14 Vulnerabilties of 5G network, extracted from [22]

Component	Vulnerability Summary
Core Network	Service-based architecture: weaknesses are related with the protection of open source APIs, in particular with their integrity, authentication and protection for the data (in transit and stored). Security update gap between new security requirements and deployment of updated versions of network functions in operational systems. Two major factors are relevant for this gap: a) vendors' responsiveness in issuing and validating new versions of the network functions that address the updated requirements, and b) timeliness and effectiveness of MNO processes to update (e.g. UDM, AUSF, SEPP, NRF, NEF, SMF, AMF and UPF). IP Based Protocol stack: the use of widely used IP protocols will lead to a shorted vulnerability exposure time and high impact of vulnerability disclosure. Besides these areas of vulnerability, virtualization vulnerabilities are also applicable, as well as generic vulnerabilities related to soft- and hardware maintenance and hardening.

Funded by Horizon Europe Framework Programme of the European Union

Component	Vulnerability Summary
Network Slicing	Security-as-a-Service: While slices provide inherent security through segmentation, slices can also be used to provide additional security protection and security services specific to the use case and customer requirements. The implementation of slice security for use cases would rest ultimately with the Mobile Network Operator (MNO) to include such services in the offer, depending on its service strategy, market context, and in relation to vertical use-cases. This might be the source of vulnerabilities, to be checked for each particular implementation. Resource isolation: While network slicing offers the ability of isolation to be used in various scenarios, the proper isolation technique has to be suited to the use case at hand. Security requirements of the particular use case will be an important element of consideration for the selection of proper isolation mechanisms. Secure Management and Orchestration: The architecture of the network slice MANO is challenging from a business model perspective. This high complexity and flexibility, which bring in higher security risks. Due to not finalized 3GPP specifications of authorisation of service management requests, implementation weaknesses may arise. Trust Model: The building of trust to MNO capabilities for the various 5G operation models has to be based on the specified APIs. It needs to be assessed, if these APIs are sufficient for all three defined operation models and how implementation will use them, in order to avoid vulnerabilities in the management functions. Besides these areas of vulnerability, virtualization vulnerabilities are also applicable, as well as generic vulnerabilities related to soft- and hardware maintenance and hardening. The following table provides a more exhaustive view on vulnerabilities of network slicing components.

Funded by Horizon Europe Framework Programme of the European Union

Component	Vulnerability Summary
Radio Access Network	Security of Ultra-Reliable Low-Latency Communication (URLLC): Weaknesses in the implementation of QoS may impact low-latency requirements. Optimization issues of control and user plane will affect reliability and low latency of communications. Vulnerability to Radio Jamming Attacks: An inherent weakness of wireless cellular communications is the free frequency space that allows for intentional or unintentional interferences. They can impact access of legitimate users and cause resilience issues in parts of the network. Failure to meet General Security Assurance Requirements: A set of weaknesses will arise through the update requirements of various elements of RAN due to implementation of migration steps and the ability of early-deployed systems to comply with specification updates regarding security functions. Optional nature of security controls for F1 interface: The optionality of security controls for this protocol may lead to security weaknesses in its implementation. Besides these areas of vulnerability, virtualization vulnerabilities are also applicable, as well as generic vulnerabilities related to soft- and hardware maintenance and hardening. The table below provides a more exhaustive view on vulnerabilities of remote access network components.
Network Function Virtualization / MANO	Management Interfaces / APIs: When developing management interfaces for the virtual functions, incomplete implementation of NVF security functions may lead to weaknesses related to access, storage and interception of network management data. Localisation of functions: While physical functions of previous mobile networks have not allowed for mobility of functions, the introduced virtualization may lead to moving virtualized functions outside their original location, notably outside the perimeter of protecting measures/policies. Besides these areas of vulnerability, virtualization vulnerabilities are also applicable, as well as generic vulnerabilities related to soft- and hardware maintenance and hardening. The following table provides a more exhaustive view on vulnerabilities of network function virtualization / MANO components.

Funded by Horizon Europe Framework Programme of the European Union

Component	Vulnerability Summary
Software Defined Networks	Control Plane: Recent practices to shift from single device controllers to distributed controllers opens doors to control plane attacks. Such attacks are based on input buffer analysis to identify forwarding policy and eventually perform manipulations based on the analysis results. Data Plane: As SDN data planes are just simple forwarding elements with no embedded intelligence, they may become targets of protocol attacks, exploiting protocol vulnerabilities in the forwarding devices. Programmable Interfaces (APIs): The Southbound API may be misused for a series of attacks. These attacks are based on inferred flow rules in SDN through packet probing. Knowing the reactive rules, attackers can launch DoS attacks by sending numerous rule-matched packets which trigger packet-in packets to overburden the controller. Besides these areas of vulnerability, virtualization vulnerabilities are also applicable, as well as generic vulnerabilities related to soft- and hardware maintenance and hardening. The table below provides a more exhaustive view on vulnerabilities of software defined networks components.
Multi-Edge Computing	Virtualization and containerization: Being based on virtualization and containerization, MEC may be vulnerable to a number of threats emerging from these technologies. Examples are: possible contamination of shared hardware resources, abuse of privilege elevation vulnerabilities of containers with higher levels of privileges, dependencies to central orchestration functions, high data and session volumes that can be subject of attacks, use of open-source APIs. Physical security: Flaws in physical security of MEC hardware may render such infrastructures vulnerable to physical attack. Given the fact of higher geographical distribution of such infrastructures, keeping a uniform level of physical security will be a challenge. Application-Programming Interfaces (APIs): Though a dedicated architecture (CAPIF) is proposed to cope with access to APIs, it has to be ensured that these provisions are followed during API design and implementation phases. As being exposed to user access, usually such APIs are subject to multiple attacks. Regulatory issues: European regulation (NIS-Directive), foresees an isolation of physical and logical components of critical services from services with low criticality. The implementation of requirement in MEC may lead to vulnerabilities of low criticality services, as they are going to be operated in a security domain with less security functions.

Funded by Horizon Europe Framework Programme of the European Union

Component	Vulnerability Summary
Physical Security	Impact of virtualisation: The physical measures/controls will need to be derived by and be complementary to weaknesses encountered by the implementation of functions in containerized and virtualized environments (see also vulnerabilities of MEC in section 4.7 above). This will mainly impact physical availability measures for the concerned functions. General physical security considerations: General physical measures need to be developed based on vulnerabilities and resulting risk-exposure that are related to the operational needs, supply chain of various components (delivery, operation, implementation, maintenance) and criticality of services. Given the large number of roles involved in 5G infrastructures, the identification of physical vulnerabilities requires a holistic approach. Threats to edge cloud computing resources: Attack surface reduction of MEC services will rely on physical measures taken for the relevant components (see also vulnerabilities in section 4.7 above). Vulnerability of wireless frequencies to jamming attacks: As a high number of wireless connections are involved in the communication within the 5G infrastructure, both in the public and non-public domain, physical measures for the reduction of impact of jamming attacks need to be taken into account, especially on availability of communication channels.
Imoplementation Options	Risks related to legacy technologies: These risks materialize through exploitation of vulnerabilities that are concerned with mismatches of functionalities of non-standalone 5G networks (NSA) to the current specifications. An example hereto are the use of the LTE Evolved Packet Core (EPC) and the LTE control panel. In this way, for NSA 5G networks, threats and vulnerabilities of the LTE technology will persist. Roaming: During migration, 4G roaming is being used for 5G. This roaming does not include the new 5G security functions, while maintaining Diameter, SIP/VoLTE and possibly SS7. These protocols are vulnerable to eavesdropping and tracking. Security update gap: Between new security requirements and deployment of updated versions of network functions in operational systems. Two major factors are relevant for this gap: a) vendors' responsiveness in issuing and validating new versions of the network functions that address the updated requirements, and b) timeliness and effectiveness of MNO processes to update. This may lead to vulnerabilities in operational NSA 5G infrastructures. Besides these areas of vulnerability, virtualization vulnerabilities are also applicable to implementation options. The table below provides a more exhaustive view on vulnerabilities of components used within 5G implementation options.

Funded by Horizon Europe Framework Programme of the European Union

Component	Vulnerability Summary
Processes	MNO processes: Security of the 5G System is achieved and maintained by upholding security objectives across the entire lifecycle of the system, in particular from the side of Mobile Network Operator (MNO). In this section, we have identified operational process weaknesses that can directly impact the security of the 5G System. As a reference model for operational processes, we used the eTOM Business Framework which defines comprehensive, industry-agreed, multi-layered view of the key business processes in the Telecommunications sector. Any other process framework could be used for this purpose. Vendor, development and product life-cycle processes: Vendor Development and Product Lifecycle covers all aspects potentially impacting a Network Product's lifetime. Vulnerabilities in vendor development and product lifecycle processes impact directly the security of 5G system components. While some vulnerabilities are directly connected to a specific phase in the Product Lifecycle, other process vulnerabilities are relevant for the entire Development and Product lifecycles. Security assurance processes: A solid and objective assessment process can contribute towards identification baseline security requirements to be met for network products and the implemented processes. This is an additional dimension to technological and operational security mitigation controls, contributing towards the assurance of their implementation levels. Following conclusions of the Toolbox, security assurance processes can only help mitigate certain risks to a limited extent given the constant need to update products and systems—making it impossible to create 'trust' through these mechanisms only. Hence, assurance processes and related measures need to be seen in combination to implementation of technical and operational ones.

Table 15 Threats of 5G network, extracted from [23]

Threat Category	Threat	Description
Core Network	Abuse of remote access	Malicious actor gains remote access to critical network components, taking control of virtual machines to perform further attacks such as configuration tampering or malware distribution.
Core Network	Authentication traffic spikes	Flood of authentication requests (e.g. from IoT devices) overwhelms the network, potentially leading to failed authentications and service denial.
Core Network	Abuse of user authentication/authorization data	Disclosure or misuse of long-term authentication keys by insiders or untrustworthy personnel in the core network.
Core Network	Abuse of third party hosted network functions	Hosting core functions on untrusted third-party clouds can lead to data disclosure, modification, or service disruption.

Funded by Horizon Europe Framework Programme of the European Union

Threat Category	Threat	Description
Core Network	Abuse of lawful interception function	Unauthorized or abusive use of lawful interception, especially when vendors/suppliers manipulate or bypass audit mechanisms.
Core Network	API exploitation	Attackers exploit poorly configured or secured APIs used throughout 5G networks to access sensitive functions or parameters.
Core Network	Poor architecture and planning	Complex or poorly implemented network design may lead to security gaps and vulnerabilities exploited by attackers.
Core Network	Exploitation of misconfigured systems/networks	Incorrect configuration (e.g. of APIs, firewalls, VNFs) provides opportunities for attackers to breach or disrupt network assets.
Core Network	Erroneous use or administration	Unintentional errors in managing devices or systems can compromise confidentiality, integrity, and availability.
Core Network	Roaming fraud	Roaming scenarios may allow illegitimate users to gain access through abuse of authentication processes.
Core Network	Lateral movement	Attackers move across network components to explore weaknesses and launch coordinated attacks.
Core Network	Memory scraping	Scanning physical memory of SDN components to extract unauthorized sensitive data.
Core Network	Network traffic manipulation	Includes tampering, injection, replay attacks, or flow priority manipulation.
Core Network	Configuration data manipulation	Tampering with routing tables, DNS records, or control data to alter network behavior or launch attacks.
Core Network	Flooding attacks	Overwhelming core components with traffic (e.g. through DDoS or amplification) to degrade or halt services.
Core Network	Traffic diversion	Rerouting traffic to unauthorized endpoints for eavesdropping or manipulation, including slice trespassing.
Core Network	Manipulation of orchestrator	Modifying orchestration settings to change function behavior and compromise service separation.
Core Network	Misuse of audit tools	Malicious insiders exploit monitoring tools to extract network data or conduct reconnaissance.
Core Network	Opportunistic use of shared resources	Leaking of AAA credentials or e2e keys by insiders allows attackers to hijack secure sessions.
Core Network	Malicious network function registration	Unauthorized NF registered to SBA to expose malicious APIs or access sensitive systems.
Core Network	Traffic sniffing	Intercepting unencrypted communication to extract critical information such as flow rules or session data.
Core Network	Side-channel attacks	Exploiting timing or flow behavior to infer internal network operations or sensitive data.
Access Network	Abuse of spectrum	Illegal use or spoofing of licensed spectrum to block or interfere with legitimate users.
Access Network	ARP poisoning	Spoofing ARP messages to redirect traffic to an attackerâ€™s system.

Funded by Horizon Europe Framework Programme of the European Union

Threat Category	Threat	Description
Access Network	Fake access node	Deploying rogue base stations (e.g. fake gNBs) to intercept or manipulate user communication.
Access Network	Flooding attacks	Overloading radio interfaces with traffic to disable or degrade wireless services.
Access Network	IMSI catching	Tracking user location or identity by exploiting paging messages and protocols like ToRPEDO.
Access Network	Jamming	Deliberate interference with radio frequencies to deny network access or GPS services.
Access Network	MAC spoofing	Forging MAC addresses to impersonate legitimate users or bypass security controls.
Access Network	Access config manipulation	Forging configuration data in access nodes to initiate other attacks like DoS.
Access Network	Radio interference	Using compromised 5G devices to interfere with wireless communication and cause DoS.
Access Network	Radio traffic manipulation	Redirecting or modifying base station traffic, often via man-in-the-middle attacks.
Access Network	Session hijacking	Stealing session tokens to take over ongoing authenticated sessions.
Access Network	Signalling fraud	Faking interconnection signaling messages to gain unauthorized access or charge manipulation.
Access Network	Signalling storms	Malicious or buggy apps generate excessive signaling traffic, overloading network components.
MEC	False or rogue gateway	Deployment of malicious edge gateways that mimic legitimate nodes for eavesdropping or attacks.
MEC	Edge node overload	Flooding edge components to exhaust local resources, often from mobile apps or IoT devices.
MEC	API abuse	Exploiting open APIs on MEC nodes to perform DoS, manipulation, or information leakage.
Virtualisation	DCI protocol abuse	Spoofing or DoS attacks exploiting vulnerabilities in data center interconnect protocols.
Virtualisation	Cloud resource abuse	Using cloud services to launch high-speed brute-force or DoS attacks.
Virtualisation	Slice bypassing	Poor isolation or misconfigurations allow cross-slice data interception or manipulation.
Virtualisation	Host abuse	Cross-tenant resource abuse or data scavenging in shared virtual environments.
Physical	Hardware manipulation	Tampering with hardware or firmware during production or maintenance by malicious suppliers.
Physical	Natural disasters	Floods, fires, and earthquakes damaging infrastructure and disrupting service availability.
Physical	Sabotage/vandalism	Physical attacks to disrupt or destroy critical infrastructure assets.
Physical	Third-party facility access	Untrustworthy contractors accessing infrastructure for maintenance can introduce risks.
Physical	UICC exploitation	Exploiting new SIM formats (eUICC, soft SIM) to launch DoS or fraud attacks.

Funded by Horizon Europe Framework Programme of the European Union

Threat Category	Threat	Description
Physical	User equipment compromise	Insecure or malicious IoT/UE devices used to compromise network security.
Generic	Denial of Service (DoS)	Flooding or exhausting network resources to block legitimate usage.
Generic	Data breach/leak/theft	Unauthorized access to or publication of personal, corporate, or state-sensitive data.
Generic	Eavesdropping	Monitoring communication traffic (including subscriber or control traffic) for sensitive data.
Generic	Software/hardware exploitation	Use of vulnerabilities (e.g., Meltdown, SS7 flaws) to compromise devices or systems.
Generic	Malicious code/software	Insertion or distribution of malware, trojans, or rogue software components.
Generic	Supply chain compromise	Malicious tampering by vendors or third-party providers before or during deployment.
Generic	Targeted threats (APT)	Advanced persistent attacks targeting intellectual property or state secrets.
Generic	Operational flaws	Poor security or operational procedures that undermine network resilience and integrity.
Generic	Authentication abuse	Theft or misuse of authentication data across network entry points or devices.
Generic	Identity spoofing	Masquerading as a legitimate entity to trigger unauthorized network behavior.

Table 16 Vulnerabilties of 5G network, extracted from [24]

Security Objective Domain	Countermeasure Description
SO01: Information security policy	Basic: a) Set a high level security policy addressing the security of networks and services b) Make key personnel aware of the security policy Industry standard: c) Set detailed information security policies for critical assets and business processes d) Make all personnel aware of the security policy and what it implies for their work e) Review the security policy following incidents State of the art: f) Review the information security policies periodically, and take into account violations, exceptions, past incidents, past tests/exercises, and incidents affecting other (similar) providers in the sector

Funded by Horizon Europe Framework Programme of the European Union

Security Objective Domain	Countermeasure Description
SO02: Governance and risk management	Basic: a) Make a list of the main risks for security of networks and services, taking into account main threats for the critical assets b) Make key personnel aware of the main risks and how they are mitigated Industry standard: c) Set up a risk management methodology and/or tools based on industry standards d) Ensure that key personnel use the risk management methodology and tools e) Review the risk assessments following changes or incidents f) Ensure residual risks are accepted by management State of the art: g) Review the risk management methodology and/or tools, periodically, taking into account changes and past incidents
SO03: Security roles and responsibilities	Basic: a) Assign security roles and responsibilities to personnel b) Make sure the security roles are reachable in case of security incidents Industry standard: c) Personnel is formally appointed in security roles d) Make personnel aware of the security roles in your organisation and when they should be contacted State of the art: e) Structure of security roles and responsibilities is regularly reviewed and revised, based on changes and/or past incidents
SO04: Security of third party dependencies	Basic: a) Include security requirements in contracts with third-parties, including confidentiality and secure transfer of information Industry standard: b) Set a security policy for contracts with third-parties c) Ensure that all procurement of services/products from third-parties follows the policy d) Review security policy for third parties, following incidents or changes e) Demand specific security standards in third-party supplier's processes during procurement f) Mitigate residual risks that are not addressed by the third party State of the art: g) Keep track of security incidents related to or caused by third-parties h) Periodically review and update security policy for third parties at regular intervals, taking into account past incidents, changes, etc.

Funded by Horizon Europe Framework Programme of the European Union

Security Objective Domain	Countermeasure Description
SO05: Background checks	Basic: a) Check professional references of key personnel (system administrators, security officers, guards, etc.) Industry standard: b) Perform background checks/screening for key personnel, when needed and legally permitted c) Set up a policy and procedure for background checks State of the art: d) Review and update policy/procedures for background checks and reference checks at regular intervals, taking into account changes and past incidents
SO06: Security knowledge and training	Basic: a) Provide key personnel with relevant training and material on security issues Industry standard: b) Implement a program for training, making sure that key personnel have sufficient and up-to-date security knowledge c) Organise trainings and awareness sessions for personnel on security topics important for your organisation State of the art: d) Review and update the training program periodically, taking into account changes and past incidents e) Test the security knowledge of personnel
SO07: Personnel changes	Basic: a) Following changes in personnel revoke access rights, badges, equipment, etc., if no longer necessary or permitted b) Brief and educate new personnel on the policies and procedures in place Industry standard: c) Implement policy/procedures for personnel changes, taking into account timely revocation of access rights, badges and equipment d) Implement policy/procedures for education and training for personnel in new roles State of the art: e) Periodically check that the policy/procedures are effective f) Review and evaluate policy/procedures for personnel changes, taking into account changes or past incidents

Funded by Horizon Europe Framework Programme of the European Union

Security Objective Domain	Countermeasure Description
SO08: Handling violations	Basic: a) Hold personnel accountable for security incidents caused by violations of policies, for example via the employment contract Industry standard: b) Set up procedures for violations of policies by personnel State of the art: c) Periodically review and update the disciplinary process, based on changes and past incidents
SO09: Physical and environmental security	Basic: a) Prevent unauthorized physical access to facilities and infrastructure and set up adequate environmental controls, to protect provider assets (including third party assets, where applicable) against unauthorized access, burglary, fire, flooding, etc. Security controls should be selected based on the risk assessment, which should also take in consideration current and forecasted environmental security risks – e.g. related to climate change Industry standard: b) Implement a policy for physical security measures and environmental controls c) Industry standard implementation of physical and environmental controls d) Apply reinforced controls for physical access to critical assets. For example, physical access to such assets should only be granted to a limited number of security-vetted, trained and qualified personnel. Access by third-parties, contractors, and employees of suppliers/vendors, integrators, should be limited and monitored State of the art: e) Evaluate the effectiveness of physical and environmental controls periodically f) Review and update the policy for physical security measures and environmental controls taking into account changes and past incidents

Funded by Horizon Europe Framework Programme of the European Union

Security Objective Domain	Countermeasure Description
SO10: Security of supplies	Basic: a) Ensure security of critical supplies Industry standard: b) Implement a policy for security of critical supplies c) Implement industry standard security measures to protect critical supplies and supporting facilities (e.g. passive cooling, automatic restart after power interruption, battery backup power, diesel generators, backup fuel, etc.) State of the art: d) Implement state of the art security measures to protect critical supplies (such as active cooling, UP, hot standby power generators, SLAs with fuel delivery companies, redundant cooling and power backup systems) e) Review and update policy and procedures to secure critical supplies regularly, taking into account changes and past incidents
SO11: Access control to network and information systems	Basic: a) Users and systems have unique ID's and are authenticated before accessing services or systems b) Implement logical access control mechanism for network and information systems to allow only authorized use Industry standard: c) Implement policy for protecting access to network and information systems, addressing for example roles, rights, responsibilities and procedures for assigning and revoking access rights d) Choose appropriate authentication mechanisms, depending on the type of access e) Monitor access to network and information systems, have a process for approving exceptions and registering access violations f) Reinforce controls for remote access to critical assets of network and information systems by third parties State of the art: g) Evaluate the effectiveness of access control policies and procedures and implement cross checks on access control mechanisms h) Access control policy and access control mechanisms are reviewed and when needed revised

Funded by Horizon Europe Framework Programme of the European Union

Security Objective Domain	Countermeasure Description
SO12: Integrity of network and information systems	Basic: a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls b) Check for malware on (internal) network and information systems Industry standard: c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems d) Apply reinforced software integrity, update and patch management controls for critical assets in virtualised networks State of the art: e) Set up state of the art controls to protect integrity of systems f) Evaluate and review the effectiveness of measures to protect integrity of systems
SO13: Use of encryption	Basic: a) Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data during its storage in and/or transmission via networks. The type and scope of data to be encrypted should be determined based on the risk assessment performed and will typically include communication data, customer critical data (e.g. unique identifiers), relevant management and signalling traffic and any other data or metadata, the disclosure or tampering of which may cause security incidents Industry standard: b) Implement encryption policy c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys State of the art: d) Review and update encryption policy e) Use state of the art encryption algorithms
SO14: Protection of security critical data	Basic: a) Make sure that cryptographic key material and secret authentication information (including cryptographic key material used for authentication) are not disclosed or tampered with Industry standard: c) Implement policy for management of cryptographic keys d) Implement policy for management of user passwords State of the art: e) Review and update of key management policy f) Review and update of user password management policy

Funded by Horizon Europe Framework Programme of the European Union

Security Objective Domain	Countermeasure Description
SO15: Operational procedures	Basic: a) Set up operational procedures and assign responsibilities for operation of critical systems Industry standard: b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures State of the art: c) Review and update the policy/procedures for operation of critical systems, taking into account incidents and/or changes
SO16: Change management	Basic: a) Follow predefined methods or procedures when making changes to critical systems Industry standard: b) Implement policy/procedures for change management, to make sure that changes of critical systems are always done following a predefined way c) Document change management procedures, and record for each change the steps of the followed procedure State of the art: d) Review and update change management procedures regularly, taking into account changes and past incidents
SO17: Asset management	Basic: a) Identify critical assets and configurations of critical systems Industry standard: b) Implement policy/procedures for asset management and configuration control State of the art: c) Review and update the asset management policy regularly, based on changes and past incidents

Funded by Horizon Europe Framework Programme of the European Union

Security Objective Domain	Countermeasure Description
SO18: Incident management procedures	Basic: a) Make sure personnel is available and prepared to manage and handle incidents b) Keep a record of all major incidents Industry standard: c) Implement policy/procedures for managing incidents State of the art: d) Investigate major incidents and draft final incident reports, including actions taken and recommendations to mitigate future occurrence of this type of incident e) Evaluate incident management policy/procedures based on past incidents
SO19: Incident detection capability	Basic: a) Set up processes or systems for incident detection Industry standard: b) Implement industry standard systems and procedures for incident detection c) Implement systems and procedures for registering and forwarding incidents timely to the appropriate people State of the art: d) Review systems and processes for incident detection regularly and update them taking into account changes and past incidents e) Implement state of the art systems and procedures for incident detection
SO20: Incident reporting and communication	Basic: a) Communicate and report about on-going or past incidents to third parties, customers, and/or government authorities, when necessary Industry standard: b) Implement policy and procedures for communicating and reporting about incidents State of the art: c) Evaluate past communications and reporting about incidents d) Review and update the reporting and communication plans, based on changes or past incidents

Funded by Horizon Europe Framework Programme of the European Union

Security Objective Domain	Countermeasure Description
SO21: Service continuity strategy and contingency plans	Basic: a) Implement a service continuity strategy for the communications networks and/or services provided Industry standard: b) Implement contingency plans for critical systems c) Monitor activation and execution of contingency plans, registering successful and failed recovery times d) Implement contingency plans for dependent and inter-dependent critical sectors and services. When determining dependent critical sectors and services, providers may take into account those services that are dependent on the continuity of the network and service operation which are essential for the maintenance of critical societal and/or economic activities and for which an incident would have significant disruptive effects on the provision of that service. One possible way for identifying such dependent services may be to pass the obligation to service consumers to inform the providers if their service is considered critical State of the art: e) Review and revise service continuity strategy periodically f) Review and revise contingency plans, based on past incidents and changes
SO22: Disaster recovery capabilities	Basic: a) Prepare for recovery and restoration of services following disasters Industry standard: b) Implement policy/procedures for deploying disaster recovery capabilities c) Implement industry standard disaster recovery capabilities, or be assured they are available from third parties (such as national emergency networks) State of the art: d) Set up state of the art disaster recovery capabilities to mitigate natural and/major disasters e) Review and update disaster recovery capabilities regularly, taking into account changes, past incidents, and results of tests and exercises

Funded by Horizon Europe Framework Programme of the European Union

Security Objective Domain	Countermeasure Description
SO23: Monitoring and logging policies	Basic: a) Implement monitoring and logging of critical systems Industry standard: b) Implement policy for logging and monitoring of critical systems c) Set up tools for monitoring critical systems d) Set up tools to collect and store logs of critical systems State of the art: e) Set up tools for automated collection and analysis of monitoring data and logs f) Review and update logging and monitoring policy/procedures, taking into account changes and past incidents
SO24: Exercise contingency plans	Basic: a) Exercise and test backup and contingency plans to make sure systems and processes work and personnel is prepared for large failures and contingencies Industry standard: b) Implement a program for exercising backup and contingency plans regularly, using realistic scenarios covering a range of different scenarios over time c) Make sure that the issues and lessons learnt from exercises are addressed by the responsible people and that the relevant processes and systems are updated accordingly State of the art: d) Review and update the exercise plans, taking into account changes, past incidents and contingencies which were not covered by the exercise program e) Involve suppliers and other third parties in exercises, for example business partners and customers
SO25: Network and information systems testing	Basic: a) Test networks and information systems before using them or connecting them to existing systems Industry standard: b) Implement policy/procedures for testing network and information systems c) Implement tools for automated testing State of the art: d) Review and update the policy/procedures for testing, taking into account changes and past incidents

Funded by Horizon Europe Framework Programme of the European Union

Security Objective Domain	Countermeasure Description
SO26: Security assessments	Basic: a) Ensure critical systems undergo security scans and security testing regularly, particularly when new systems are introduced and following changes Industry standard: b) Implement policy/procedures for security assessments and security testing State of the art: c) Evaluate the effectiveness of policy/procedures for security assessments and security testing d) Review and update policy/procedures for security assessments and security testing, taking into account changes and past incidents
SO27: Compliance monitoring	Basic: a) Monitor compliance to standards and legal requirements Industry standard: b) Implement policy/procedures for compliance monitoring and auditing State of the art: c) Evaluate the policy/procedures for compliance and auditing d) Review and update the policy/procedures for compliance and auditing, taking into account changes and past incidents
SO28: Threat intelligence	Basic: a) Perform regular threat monitoring Industry standard: b) Implement threat intelligence program State of the art: c) Review and update the threat intelligence program d) Threat intelligence program makes use of state of the art threat intelligence systems
SO29: Informing users about threats	Basic: a) Inform end-users of communication networks and services about particular and significant security threats to network or service that may affect them Industry standard: b) Implement policy/procedures for regular update of end-users about security threats to network or service that may affect them State of the art: c) Review and update the policy/procedures for regular update of end-users about security threats to network or service that may affect them

Funded by Horizon Europe Framework Programme of the European Union

Funded by Horizon Europe Framework Programme of the European Union

Appendix D. Blockchain Cybersecurity

The list of vulnerabilities, threats and countermeasures were extracted from [25].

Table 17 Vulnerabilties of 5G network, extracted from [25]

Vulnerability	Description
Key Management	Private keys are the direct means of authorizing activities from an account. If accessed by an adversary, they compromise any wallets or assets secured by these keys.
Cryptography	Challenges in managing cryptographic keys properly, including weaknesses in key generation, potential quantum computing threats, and issues with random number generators.
Privacy	Permissionless ledgers allow all counterparties to download the ledger, potentially exposing transaction history. The 'right to be forgotten' is difficult to implement.
Code Review	Despite review efforts, vulnerabilities and zero-day attacks in Blockchain protocols and applications may still exist.
Consensus Hijack	In decentralized networks, an attacker controlling a large portion of participating clients could manipulate transaction validation (e.g., 51% attack).
Sidechains	Sidechains may have weaker security than their parent chains, making them vulnerable to fraudulent transactions and potential exploitation.
Exploiting Permissioned Blockchains	In a regulated network, if the entity managing the system is compromised, it could allow severe exploitation.
Distributed Denial of Service (DDoS)	Rogue wallets can spam the network with large volumes of transactions, causing delays and service disruptions.
Wallet Management	The security of wallets is crucial; compromised keys may lead to irreversible asset loss with no way to detect breaches until too late.
Scalability	The size and speed of Blockchain transactions may create storage and processing issues as ledgers grow.
Smart Contract Management	Smart contracts are prone to bugs and vulnerabilities, and poorly written contracts may lead to exploits (e.g., Ethereum DAO hack).
Interoperability	Different Blockchain ledgers have difficulty exchanging data due to differences in protocols, transaction formats, and governance rules.
Governance Controls	Institutions still require governance structures to regulate financial transactions and prevent unauthorized activities.
Anti-Fraud and Anti-Money Laundering Tools	Blockchain lacks sufficient tools for fraud detection and AML compliance, making illicit activities difficult to prevent proactively.

Table 18 Threats of 5G network, extracted from [25]

Threat	Description
Double Spending	Occurs when a single digital token is spent more than once due to vulnerabilities in consensus mechanisms.

Funded by Horizon Europe Framework Programme of the European Union

Threat	Description
Selfish Mining	A type of attack where miners withhold discovered blocks to gain an unfair advantage and control the mining process.
Sybil Attack	An attacker creates multiple fake identities to gain influence and disrupt the blockchain network.
Routing Attack	Intercepting blockchain network traffic to delay or manipulate transactions and block propagation.
Eclipse Attack	An attacker isolates a node by controlling its incoming and outgoing connections, feeding it false information.
51% Attack	If an entity controls more than 50% of a blockchain's mining power, they can manipulate transactions and double-spend.
Smart Contract Vulnerabilities	Bugs and loopholes in smart contract code can be exploited, leading to security breaches and fund theft.
Private Key Theft	The theft or loss of private keys results in irreversible loss of assets and control over accounts.
Consensus Algorithm Weaknesses	Flaws in consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS) can lead to network manipulation.
Unauthorized Forking	Malicious actors can create unauthorized forks of blockchain networks, causing confusion and splitting communities.

Table 19 Countermeasures of 5G network, extracted from [25]

Category	Challenges	Good Practices
Key Management	key storage, key loss, key theft	- Store keys according to good practices
		- Use rules that require the use of multiple signatures to authorize and/or create transactions
		- Allow the use of recovery agents – one way of doing this is through a trusted third party which holds, the keying material required to recover keys
		- Use different keys to sign and encrypt
		- Enable internal identification of the individual signing off the request for a transaction
		- Issue individual keys to persons working on behalf of institution
Cryptography	Key generation	- Make sure the keys are generated in a secure and valid way
		- Make sure the key length is appropriate for the use
		- Use different keys to sign and encrypt
Privacy	Keep information visible only to authori-	- Encrypt the transactions, so only the involved counterparties can access the whole information

Funded by Horizon Europe Framework Programme of the European Union

Category	Challenges	Good Practices
	zed entities, Unauthorized access to transactions	- Use sharding to allow specific transactions to be validated by specific entities
		- Use pruning to remove data from the ledger at certain period of time, as requested by the regulation
		- In case an entity must be linked to a key, an authority may keep information of which key belongs to which entity
		- Encrypt ledger with more than one key
Code Review	Bugs/Errors, Zero-day attacks	- Do code review (or employ third party services) of Blockchain applications and associated libraries
		- Apply Software Development Life Cycle principles
		- Do penetration testing (or employ third party services) of the Blockchain application
Consensus Hijack	Fraudulent transactions	- Monitor if one of the nodes increases processing power and is executing a significantly higher number of transactions
		- Assign fees to new transactions or make it difficult for a node to process a large number of transactions
Sidechains	Fraudulent transactions	- Require the use of merged mining, where the proof of work applied to validate the parent chain may also be used to submit valid blocks for the sidechain
Permissioned Chain Mgmt	Central authority key loss, A node getting enough power to validate transactions of their choice – potentially fraud	- Monitor if one of the nodes increases processing power and is processing a significantly higher number of blocks
		- Use a clear set of criteria to accept new members, as well as to remove existing ones
		- Enable the use of recovery keys
Denial of Service	Spam/invalid transactions being introduced for validation, Slow processing of transactions	- Restrict which nodes can offer new transactions for validation
		- Assign fees to new transactions or make it difficult for a node to issue large numbers of transactions
		- Accept transactions from only authorized IP addresses

Funded by Horizon Europe Framework Programme of the European Union

Category	Challenges	Good Practices
		- Have the possibility to block IP addresses as necessary
Wallet Management	Key theft, Unauthorized access to data, Information disclosure, Block/Compromise of operations of entity	- Make sure the software for the wallet does not leave the key accessible in plain text outside the application
		- Require the implementation of recovery keys
Scalability	Slow processing of transactions, Unexpected growth of the distributed ledger database	- Use sharding to allow specific transactions to be validated by specific entities
		- Use pruning to limit the growth of the ledger
		- Restricting the type of information allowed on the ledger and the entities allowed to act as full nodes
Governance Controls	Institutions engaging in a not permitted activity	- Use smart contracts to allow for certain entities to engage in certain activities
		- Internal governance procedure must enable internal identification of the individual signing off the request
Smart Contracts	Unwanted behaviour of smart contracts, Malicious software spread	- Use code review for smart contracts
		- Standardization of regular functions into libraries
		- Keep a library of approved smart contracts
		- Participants could use consensus protocol which considers a malicious program as an invalid state
Interoperability	Fraudulent transactions	- Use pegged sidechains

Funded by Horizon Europe Framework Programme of the European Union

Appendix E. Artificial Intelligence Cybersecurity

The list of vulnerabilities, threats and countermeasures for Artificial Intelligence were derived from [26].

Table 20 Vulnerabilties of AI, extracted from [26]

Vulnerability	Description
Vulnerable Software Design	AI systems may have design flaws that expose them to adversarial attacks, data poisoning, and privacy risks. Poorly architected models can allow attackers to manipulate outputs or gain unauthorized access to sensitive data.
Vulnerable or Outdated Components	AI models often rely on third-party libraries, datasets, or pre-trained models that may be outdated or insecure. These outdated dependencies can introduce vulnerabilities that attackers can exploit.
Broken or Weak Access Control	Insufficient access control mechanisms can allow unauthorized users to manipulate AI models, extract sensitive training data, or execute adversarial attacks against the system.
Third-Party Risks	AI systems often integrate third-party components, data sources, or software tools that may introduce security vulnerabilities, data biases, or regulatory compliance risks.
Lack of Explainability and Transparency	AI systems that lack transparency and interpretability can make it difficult to detect biases, security flaws, or unintended behaviors, increasing overall risk exposure.
Training Data Leakage	AI models may inadvertently expose confidential or personal information contained in their training datasets, leading to privacy and security concerns.
Unsecured Model APIs	Publicly accessible AI APIs can be exploited by attackers to extract model parameters, manipulate outputs, or launch adversarial attacks.
Bias and Fairness Risks	AI models trained on biased data can produce discriminatory outcomes, leading to ethical, legal, and reputational risks.
Lack of Robustness to Concept Drift	AI models may fail to adapt to changes in data distributions over time, making them unreliable in dynamic environments.
Weak Encryption and Data Protection	Inadequate encryption and security mechanisms can expose AI model data to unauthorized access and manipulation.
Insufficient Monitoring and Logging	A lack of proper monitoring and logging mechanisms can prevent organizations from detecting AI system anomalies, security incidents, or adversarial attacks.
Security Misconfigurations	Weak security settings in AI systems expose them to unauthorized access, manipulation, or exploitation by attackers.
Untrusted Third-Party Dependencies	AI models that rely on external datasets, libraries, or APIs may introduce security vulnerabilities if those dependencies are compromised.
Compromised AI Ethics and Governance	Weak governance and ethical controls can lead to AI misuse, discrimination, or unethical decision-making processes.

Funded by Horizon Europe Framework Programme of the European Union

Table 21 Threats of AI, extracted from [26]

Threat	Description
Adversarial Attacks	Attackers manipulate AI inputs in subtle ways to cause incorrect outputs, leading to misclassification, system failure, or security breaches.
Data Poisoning	Malicious actors introduce corrupted or biased data into training datasets to degrade AI model performance or introduce exploitable weaknesses.
Model Inversion Attacks	Attackers reconstruct parts of the AI training dataset by repeatedly querying the model, leading to data leakage and privacy violations.
Membership Inference Attacks	An adversary determines whether a specific data point was used in training the model, which can reveal sensitive information about individuals.
Model Stealing	Attackers reconstruct an AI model by repeatedly querying it and analyzing its outputs, effectively replicating its functionality without authorization.
Bias Exploitation	Malicious actors manipulate AI systems by exploiting biases inherent in the model's training data, potentially leading to unfair or harmful decisions.
Data Leakage	Sensitive information from AI training data inadvertently gets exposed, either through model outputs, adversarial queries, or insecure data storage.
Evasion Attacks	Attackers craft inputs designed to bypass AI security measures, allowing them to avoid detection in fraud, malware classification, or facial recognition systems.
Denial of Service (DoS) on AI Systems	Attackers overwhelm AI systems with excessive queries or adversarial inputs, degrading performance and causing downtime.
AI-generated Misinformation	Malicious entities use AI to generate misleading or harmful content, such as deepfakes, propaganda, or fake news.
Automated Phishing Attacks	Cybercriminals use AI-generated emails or messages to impersonate trusted sources and trick users into divulging sensitive information.
AI-assisted Cybercrime	Adversaries leverage AI to automate cyberattacks, improving their efficiency and effectiveness in bypassing security defenses.
AI Supply Chain Attacks	AI systems can be compromised through vulnerabilities in the supply chain, such as tampered hardware, software, or datasets.
Concept Drift Exploitation	Attackers exploit AI models that fail to adapt to evolving data distributions, leading to incorrect predictions or degraded performance.

Table 22 Countermeasures for AI, extracted from [26]

Countermeasure	Description
AI System Security and Resilience	Evaluate and document security and resilience measures to ensure AI systems can withstand unexpected adverse events and attacks.
Red-Teaming Exercises	Use red-team exercises to actively test the system under adversarial or stress conditions, measure system response, assess failure modes, and determine if the system can return to normal function after unexpected events.
Continuous Security Testing	Establish and track AI system security tests and metrics (e.g., incident response times, anomalous events, system downtime).

Funded by Horizon Europe Framework Programme of the European Union

Countermeasure	Description
Authentication and Access Control	Implement strong authentication and access control measures to prevent unauthorized system manipulation or data extraction.
Throttling and Rate Limiting	Use throttling mechanisms to prevent automated attacks and excessive API requests.
Differential Privacy	Apply differential privacy techniques to limit the risk of data leakage from AI models.
Robust Machine Learning Techniques	Employ robust ML techniques such as adversarial training and certified defenses to mitigate attacks.
Model Watermarking	Utilize watermarking technologies as a deterrent to data and model extraction attacks.
Secure Model APIs	Ensure AI model APIs are secured with proper authentication, encryption, and monitoring to detect misuse.
Data Governance Policies	Implement robust data management policies to prevent unauthorized access and ensure data integrity.
Explainability and Transparency	Develop explainability and transparency mechanisms to help detect biases, anomalies, and adversarial behavior in AI models.
Third-Party Security Audits	Require third-party AI resources and personnel to undergo security audits and screenings to prevent supply chain threats.
Incident Response Planning	Develop and document incident response plans for AI-related security threats.
AI Model Version Control	Maintain strict version control of AI models and track changes to detect unauthorized modifications.
Federated Learning	Use federated learning to minimize the need for centralized data storage and reduce exposure to data breaches.
Ethical AI Governance	Establish policies and frameworks for responsible AI development, addressing fairness, accountability, and transparency.
Secure AI Supply Chain	Verify and manage security risks associated with third-party AI components, datasets, and dependencies.
Monitoring and Logging	Implement comprehensive logging and monitoring mechanisms to detect unusual behavior and attacks on AI systems.
Regulatory Compliance	Ensure AI systems comply with relevant legal and regulatory frameworks for security and privacy.

Funded by Horizon Europe Framework Programme of the European Union