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

D4.1 CMD Risk Management Methodologies

Revision: v.1.0

Work package	WP 4
Task	Task 4.1
Due date	30/11/2023
Submission date	30/11/2023
Deliverable lead	INOV
Version	1.0
Authors	João Rodrigues (INOV), Gonçalo Cadete (INOV)
Reviewers	Pietro Di Maggio (MCI), Andrea Scaburri (MCI), Simone Favrin (MCI)

Abstract	This document reports the risk management methodologies that are most relevant for the Connected Medical Devices context and documents the challenges and requirements for next-generation risk management tools gathered on interviews performed to the CYLCOMED partners.

Keywords	Connected Medical Devices, Risk Management Framework, Cybersecurity, Safety, Threat, Risk, Vulnerability, Risk Treatment

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V0.1	20/11/2023	First Issue	INOV
V0.2	22/11/2023	Revision	MCI
V0.3	22/11/2023	Revision	Charite
V1.0	29/11/2023	Reviewers' comments and suggestions incorporated	INOV

Disclaimer

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

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

Copyright notice

Project co-funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	R	
Dissemination Level		
PU	*Public, fully open, e.g. web*	**x**
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

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

Funded by Horizon Europe Framework Programme of the European Union

Executive summary

This document reports the risk management methodologies that are most relevant for the Connected Medical Devices context and documents the challenges and requirements for next-generation risk management tools gathered on internal interviews performed with the CYLCOMED partners.

In this report, a brief description is given for the risk management frameworks that are:

- Most recognized internationally, and that are used in or mapped into other frameworks;
- The German, Italian and Spanish official cybersecurity risk management frameworks;
- Relevant for Connected Medical Devices;
- Used by the CYLCOMED partners.

This report also introduces the result of the CYLCOMED partners view on the challenges and requirements they see in the emergent technologies that need to be reflected in the CYLCOMED risk management process to be designed.

Funded by Horizon Europe Framework Programme of the European Union

Table of contents

Funded by Horizon Europe Framework Programme of the European Union

List of figures

Funded by Horizon Europe Framework Programme of the European Union

List of tables

No table of figures entries found.

Funded by Horizon Europe Framework Programme of the European Union

Abbreviations

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 Authonomous 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
GAIA-X	Project for Federated secure data infrastructure for europe, referencing the Greek goddess Gaia
GDPR	General Data Privacy Regulation
IDSA	International Data Spaces Association
IEC	International Electrotechnical Commission
IND	Industrial IT
INF	Infrastructure
IoMT	Massive 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 regulation
MDR	Medical Device
MEC	Multi-access Edge Computing
mMTC	Massive Machine-type Communication
NET	Networks and Communication
NIST	National Institute for Standards and Technology
OPS	Operations
ORP	Organisation and Personnel
OWASP	Open Web Application Security Project
PDCS	Plan, Do, Check, Act process cycle
POS	Proof Of Stake
POW	Proof of Work
RMF	Risk Management Framework
SaMD	Software as a Medical Device

Funded by Horizon Europe Framework Programme of the European Union

SIEM	Security Information and Event Management
SYS	IT System
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

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 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 framework for connected medical devices will be designed, taking into account:

- The risk management frameworks that are most relevant for connected medical devices;
- The cybersecurity risk management frameworks of the CYLCOMED partner's country hospital sites (Germany, Italy and Spain);
- The risk framework followed by the CYLCOMED partners that are suppliers of technological solutions for healthcare;
- Emerging technologies, like 5G, Blockchain, Cloud services, Artificial Intelligence, and IoT, where the CMDs are included;
- The CYLCOMED partners' continuous interaction throughout the project, in order to identify needed requirements, adaptations to new regulations and frameworks that are being prepared by standardization organizations, and any other relevant aspects that are deemed important to the project.

This report focuses on the risk management frameworks that are:

- Most recognized internationally, and that are used in or mapped into other frameworks;
- The German, Italian and Spanish official cybersecurity risk management frameworks;
- Relevant for Connected Medical Devices;
- That are used by the CYLCOMED partners.

Funded by Horizon Europe Framework Programme of the European Union

This report also introduces the CYLCOMED partners view on the challenges and requirements they see in the emergent technologies that need to be reflected into the CYLCOMED risk management process to be designed.

1.1 Methodology

For elaborating this report, the following methodology was followed (Figure 1):

- First, an extensive survey on existing risk management frameworks and standards was conducted. At the same time, the emerging technologies security standards, methodologies, risk management frameworks and standards were surveyed;
- Then, a preparation phase for the interviews to be carried out with the CYLCOMED partners was initiated;
- Then a set of interviews with the Cylcomed project's partners was performed in order to gather information on what risk management methodologies and their views, concerns and recommendations for the emerging technologies (IoT devices, AI, Cloud, 5G and Blockchain);
- Afterwards, an analysis of the interviews was performed;
- Finally, this report was prepared.

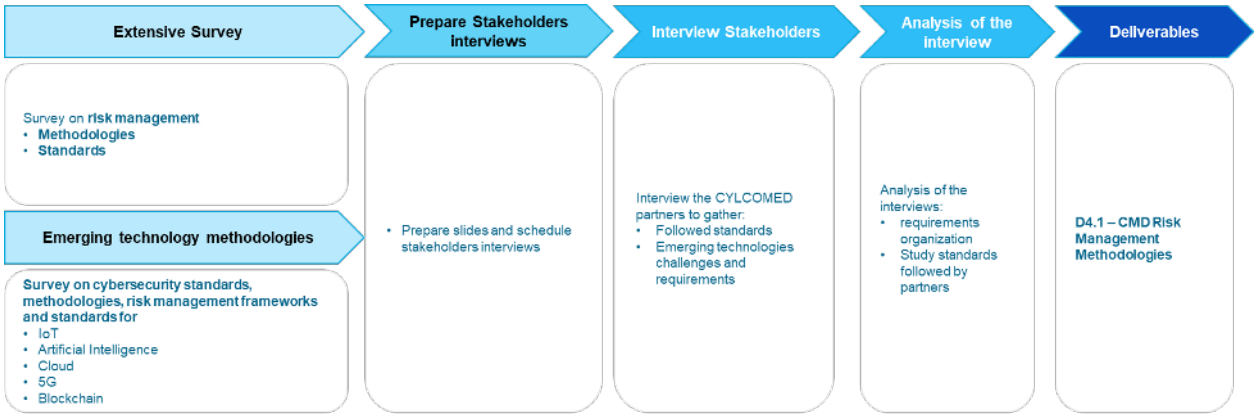

Figure 1 Methodology for elaboration of this report

1.2 Structure of the document

The document is structured as follows:

Section 2 is dedicated to a brief description to risk management;

- Section 3 describes, among these, the frameworks with greater international recognition, and that are used or mapped into other frameworks;
- Section 4 describes some aspects of the German, Italian and Spanish official cybersecurity risk management frameworks;
- Section 5 presents the CYLCOMED partners view on the challenges and requirements they see in the emergent technologies that need to be reflected in the CYLCOMED risk management process to be designed.
- The final section is reserved for the conclusions.

Funded by Horizon Europe Framework Programme of the European Union

2 Introduction to 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 2.

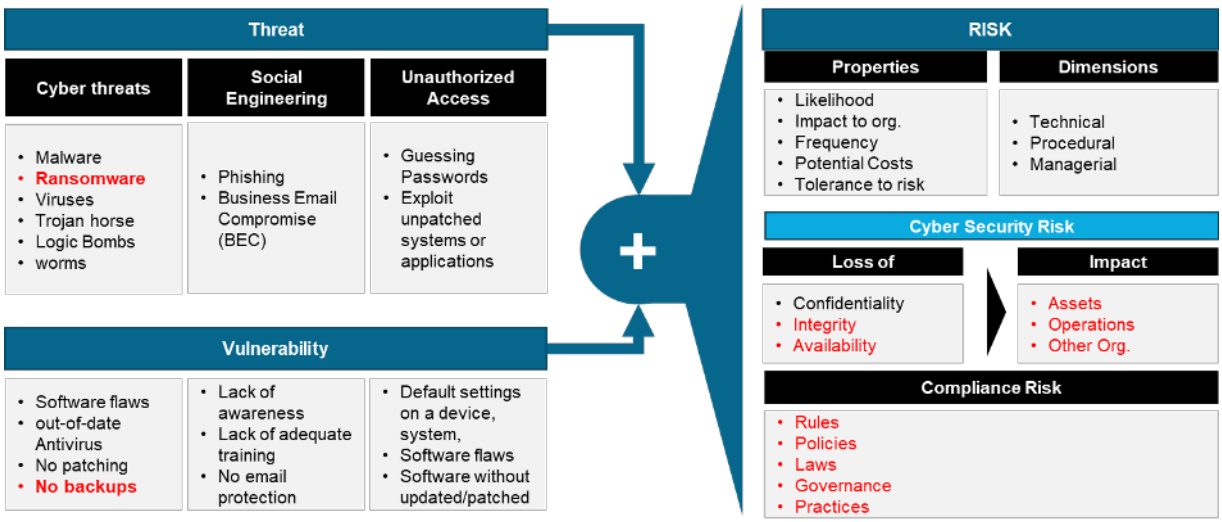

Figure 2 Relationship between threat, vulnerability and risk with some examples in the context of cybersecurity. An example of combination of a threat and vulnerabilities, and potential impact areas are marked in red

If an organization has no backup mechanisms in place (vulnerability), then 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 to the organization;
- Frequency;
- Potential costs;
- The organization's tolerance to risk.

Funded by Horizon Europe Framework Programme of the European Union

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 [1]. 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 on risk management guidance, risk management has the following 5 stages [2], [3], [4]:

- **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, risk analysis and risk evaluation. Risk identification 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 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. Finally, the risk evaluation phase, 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 and 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 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.

[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

3 Internationally Recognized Standards

3.1 Information System Specific Risk Management Framework

The field of cybersecurity includes not only technical tools to protect the digital assets, but also includes processes, procedures, and also managerial and governance aspects in order to manage the cybersecurity risks. Many cybersecurity risk management frameworks and standards exist nowadays. Cybersecurity risk management frameworks must be carefully adopted into the context the organization is in, for better utilization of resources to control the risks the organization faces, and to better planning of activities to guarantee cybersecurity.

In this section, a brief description of the most relevant standards studied, up to now, is given.

3.1.1 ISO/IEC 27001 and ISO/IEC 27002

ISO/IEC 27001 is the world's best-known standard for information security management systems (ISMS) and their requirements. Additional best practice in data protection and cyber resilience are covered by more than a dozen standards in the ISO/IEC 27000 family. Together, they enable organizations of all sectors and sizes to manage the security of assets such as financial information, intellectual property, employee data and information entrusted by third parties. ISO/IEC 27000 and the other standards in the family have been developed by the ISO/IEC joint technical committee JTC 1, or more precisely its subcommittee 27 on Information security, cybersecurity and privacy protection [5].

ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS) within an organization [6].

The ISO 27001 follows a process approach, named the Plan-Do-Check-Act (PDCA) approach [7], where:

- PLAN stage's objective is to establish the ISMS and comprises activities for establishing the context of the organization, establishing leadership for the ISMS, and the risk treatment process for the ISMS, where the information security controls present in the ISO27001 ANNEX A must be considered;
- DO stage's objective is to implement and operate the ISMS and comprises information security activities related to human resources and skill needed for operating the ISMS and the implementation and operation of the procedures defined in the PLAN stage to achieve the defined objectives;
- CHECK stage's objective is to Monitor and Review the ISMS and includes activities for monitoring, analyzing and evaluating the ISMS, audits and management reviews;
- ACT stage's objective is to maintain and improve the ISMS and includes activities for taking corrective actions and for continual improvement of the ISMS.

The PDCA stages and the ISO 27001 clauses matching is schematized in Figure 3.

Funded by Horizon Europe Framework Programme of the European Union

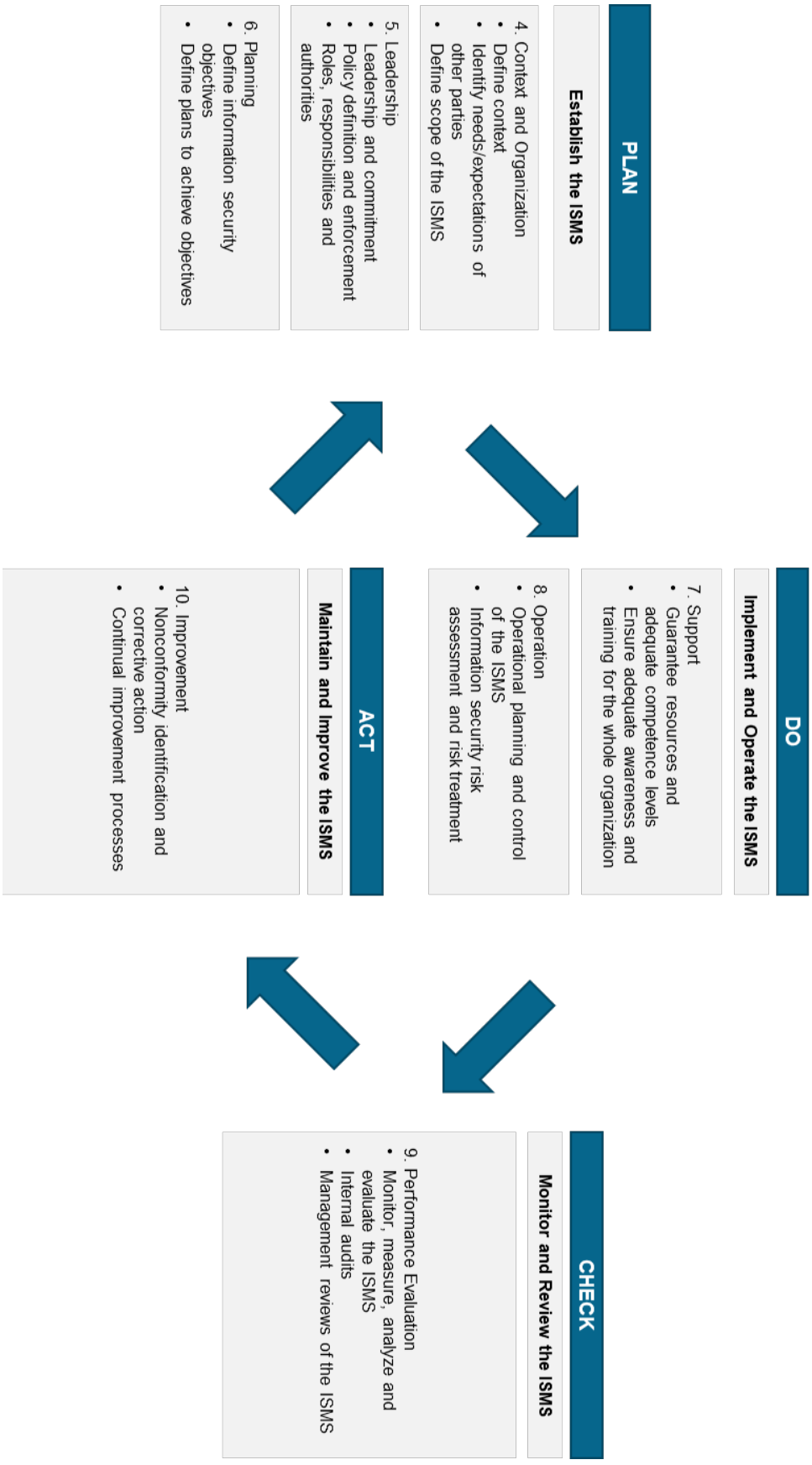

Figure 3 Illustration of the ISO/IEC 27001:2022 and its relation to the PDCA stages [8]

Funded by Horizon Europe Framework Programme of the European Union

During the PLAN stage, when defining the risk treatment process, the organization must justify the risk treatment control options that are most appropriate. The risk treatment process must be documented in:

- a document called the Statement of Applicability;
- the risk treatment plan.

The controls of Annex A covers organization controls, people controls, physical controls and technological controls, as shown in Figure 4.

Funded by Horizon Europe Framework Programme of the European Union

Figure 4 Controls area in the 2022 version of ISO 27001 [9]

Funded by Horizon Europe Framework Programme of the European Union

Further guidance on implementing the Annex A controls can be found on ISO 27002 standard.

ISO 27701 extends the ISO 27001 and ISO 27002 standards for privacy information management [10].

3.1.2 NIST Risk Management Framework

The National Institute of Standards and Technology (NIST) is part of the United States Department of Commerce. Its mission is to “promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology” [11].

In the context of cybersecurity, NIST develops cybersecurity standards, best practices, and other resources, driven by the needs of the U.S. industry. They engage with stakeholders to prioritize their activities towards addressing the U.S. industry needs and issues [12].

The NIST Special Publication 800-37, Risk Management framework for Information Systems and Organizations (NIST RMF), describes a framework for managing security and privacy risks, following a system life cycle approach.

The NIST RMF describes seven essential stages are shown in Figure 5.

Funded by Horizon Europe Framework Programme of the European Union

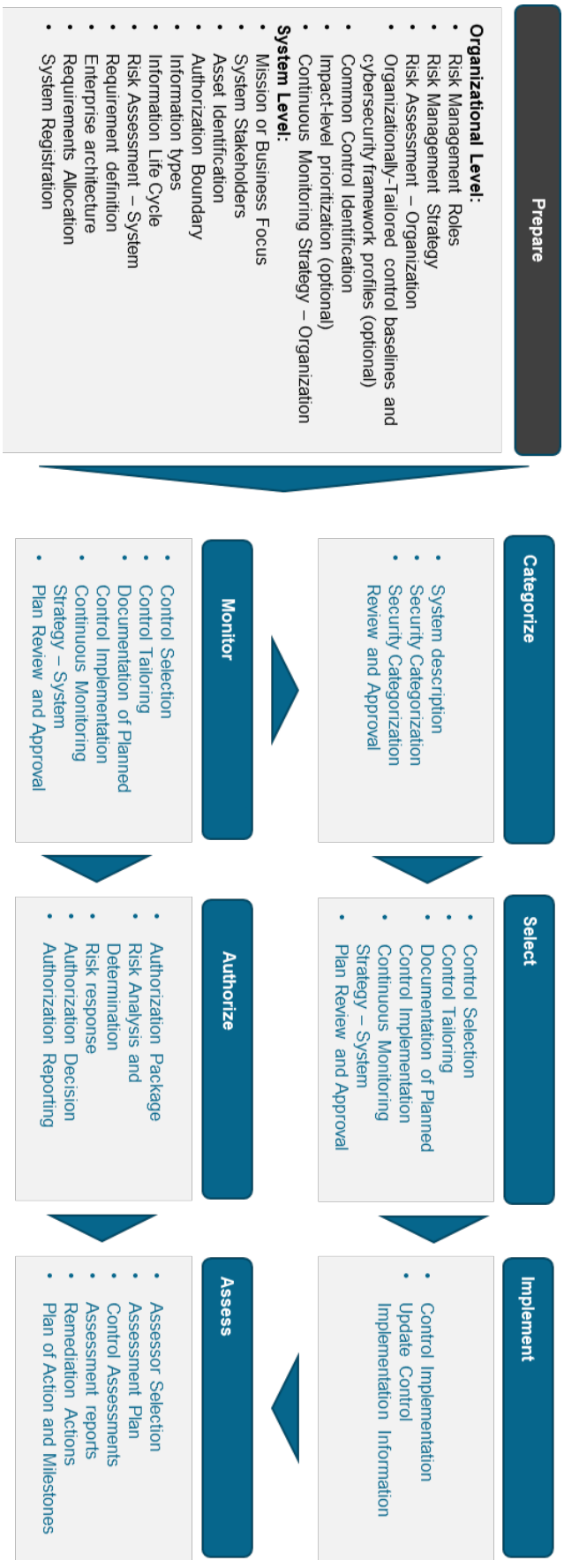

Figure 5 NIST RMF stages

Funded by Horizon Europe Framework Programme of the European Union

In the Prepare stage, the organization establishes its' context and priorities for managing the security risks, identifying the risk management roles, strategies, relevant assets within the determined scope. In this stage the continuous monitoring strategies for the risk management process are also defined.

In the Categorize stage, the risk analysis is performed in each of the asset that are relevant for the determined context. Impact levels are assign for each identified risk, resulting in a security categorization of the assets.

With the assets security categorization, the organization can move on to the Select stage where it can select the most appropriate controls for treating the identified risks. These controls could be determined from any context relevant standard, like ISO 27001/27002 or NIST CSF. Monitoring procedures are also selected, during this stage, to determine the effectiveness of the selected controls (e.g., audits, logging systems/procedures/data).

The implement stage is where the organization implements the selected controls. Note that during the implementation of the control mechanisms, unforeseen difficulties or changes might arise. For this reason, an update of the control implementation data is also included in the activities of this stage.

In the Assess stage, the implemented controls are subject to assessment for determining their effectiveness and any corrective actions that might be needed for guaranteeing the required level of security. To this end, the individuals performing these types of assessments should be carefully selected to guarantee impartiality.

The Authorization stage concerns with the executive authorizations regarding the performed risk analysis, controls selections, risk levels, and permissions for any activities related to the risk management process.

The Monitor stage ensures that the overall risk management system is functioning properly.

3.1.3 NIST Cybersecurity Framework

The NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF) describes a risk process for managing risks, has three components [13]:

- The **Framework Core**, which organizes activities for ongoing cyber risk management. They are organized in 5 categories: Identify; Protect; Detect; Respond and Recover. Each category contains subcategories with specific activities/controls.
- The **Framework Profiles**, which result from the selection of the needed Framework Core activities, according to the business objectives of the organization, the threat environment and the determined requirements.
- The **Implementation Tiers**, which specifies the maturity of the cybersecurity risk management framework.

Funded by Horizon Europe Framework Programme of the European Union

Framework Core

Identify Context		Protect Assets		Detect Anomalies		Respond to Incidents		Recover From Incidents	
ID.AM	Asset Management	PR.AC	Protect assets by managing access	DE.AE	Detect anomalies by analyzing events	RS.RP	Respond to incidents by controlling steps	RC.RP	Recover from incidents by controlling steps
ID.BE	Business Environment	PR.AT	Protect assets by managing awareness	DE.CM	Detect anomalies by monitoring systems	RS.CO	Respond to incidents by coordinating action	RC.IM	Recover from incidents by making improvements
ID.GV	Governance	PR.DS	Protect assets by managing data security	DE.DP	Detect anomalies by maintaining processes	RS.AN	Respond to incidents by analyzing the situation	RC.CO	Recover from incidents by coordinating activities
ID.RA	Risk Assessment	PR.IP	Protect assets by managing information			RS.MI	Respond to incidents by mitigating the damage		
ID.RM	Risk Management Strategy	PR.AM	Protect assets by managing maintenance			RS.IM	Respond to incidents by making improvements		
ID.SC	Supply chain	PR.PT	Protect assets by managing technologies						

Figure 6 NIST CSF Framework Core categories and subcategories

Framework Profiles

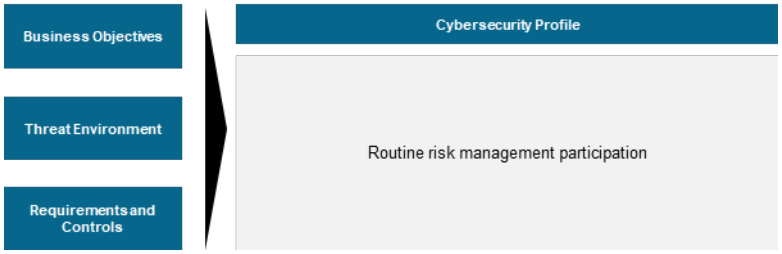

Figure 7 NIST CSF Framework Profile

Implementation Tiers

TIERS	Description	Processes	Programs	Risk management participation
TIER 4	Adaptive Risk Management Methods	Dynamic risk management processes	Responsive risk management programs	Interactive risk management participation
TIER 3	Structured Risk Management Methods	Orderly risk management processes	Robust risk management programs	Routine risk management participation
TIER 2	Informal Risk Managment Methods	unfinished risk management processes	underdeveloped risk management programs	Incomplete risk management participation
TIER 1	Ineffective Risk Management Methods	Unsystematic risk management processes	Unreliable risk management programs	unresponsive risk management participation

The Identify category encompasses activities for understanding the organizational context; for inventorying the assets supporting the organizations' business activities; activities for planning the cybersecurity protection; activities for identifying roles and responsibilities; activities for understanding and documenting the interdependencies with other organizations (e.g., analysing the supply chain); activities for identifying cybersecurity risk levels and risk management strategies.

The Protect category comprises technical and non-technical security controls to guarantee a minimum level of protection required for guaranteeing the risk management strategies.

Technical security controls include:

- Audit log systems;
- Protection against media removal;
- Security controls for networks and all type of communications

Funded by Horizon Europe Framework Programme of the European Union

- Resilience mechanisms (load balancing mechanisms, failsafe mechanisms, redundant energy supply);
- Data protection mechanisms (encryption, data leak protections, data integrity controls);
- Identity and access management controls;
- Systems supporting backup;
- Systems supporting baseline configurations (that incorporating security principles).

Non-technical activities include:

- Definition and enforcement of the security policies (detailing the purposes, scope, roles, responsibilities, management commitment, and coordination among organizational entities);
- Backup processes;
- Baseline configuration procedure and processes;
- Data elimination processes, including safe disposal of both paper-based and digital information;
- Awareness and training activities, which can include training classes, e-learning and certifications according to roles and responsibilities, phishing campaigns, awareness posters and screensavers;
- Maintenance procedures and processes for the industrial controls and information system components.

Other activities include:

- Vulnerability management;
- Incident response;
- Disaster recovery;
- Business continuity planning;
- Testing activities for the above-mentioned plans.

Even with the protective controls, cybersecurity incidents can occur. For that reason, the **Detect category** includes monitoring activities, such as periodic audit log analysis, internal and external auditing, or any technology, process or procedure that enables the detection of any event that can potentially lead to a cybersecurity incident.

The Respond category encompasses activities for responding to an incident, when it is detected. It includes activities such as incident data analysis, coordination and relevant data sharing among the appropriate personnel within the organization, and with external stakeholders (including law enforcement agencies, technology suppliers) in order to synchronize an appropriate and timely response to the incident. Once the incident is contained, and its effects mitigated, the incident must be documented.

After a cybersecurity event is contained and its effects mitigated/eliminated, activities for restoring the normal functioning of systems and processes takes place. Activities related to recovery are captured in the **Recover category**. It includes the execution of the recovery plan, continuous improvements activities of the organization's cybersecurity risk management like incorporating lessons learned from incidents into the recovery planning and training updates.

The NIST CSF risk management process is systematized in Figure 8 and is composed of seven steps:

- **Prioritize**, where the organization identifies it's business/mission objectives, priorities and risk tolerance and determines the scope of the cybersecurity risk management process.
- **Orient**, where the organization identifies, within the defined context (determined in the Prioritize phase), processes, systems, assets regulatory requirements that are crucial for the security objectives. The risk approach is defined in this stage as well.

Funded by Horizon Europe Framework Programme of the European Union

- **Create Current Profile** of the organization, based on the Framework Core and the maturity level;
- **Conduct Risk Assessment**, where the operational environment is analysed, the likelihoods of cybersecurity events are determined and their impacts are evaluated.
- **Create Target Profile**, which represents the organization's desired level of cybersecurity;
- **Determine, Analyse and Prioritize Gaps**, where the organization performs a gap analysis between the current cybersecurity profile and the target cybersecurity profile, evidencing what needs to be done. Then, the organization prioritizes the activities to achieve the target profile and designs a plan and determine the necessary resources to address the gaps.
- **Implement the Action Plan**, where the organization determines the activities needed to address the gaps and implement them.

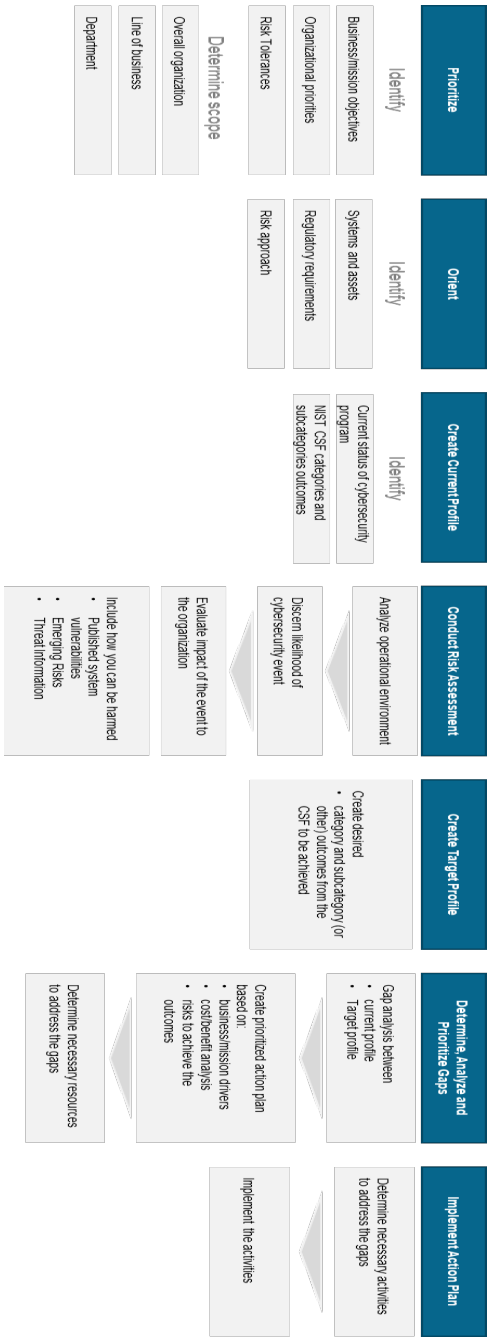

Figure 8 NIST CSF risk management process steps

Funded by Horizon Europe Framework Programme of the European Union

3.1.4 NIST Privacy Management Framework and AI Risk Management Framework

Other identified NIST frameworks that are relevant for the Cylcomed project are the NIST Privacy Management Framework and the AI Risk Management Framework. They follow closely the structure and methodology of the NIST CSF, but differ in the Framework Core. You can find it in Figure 9 and Figure 10.

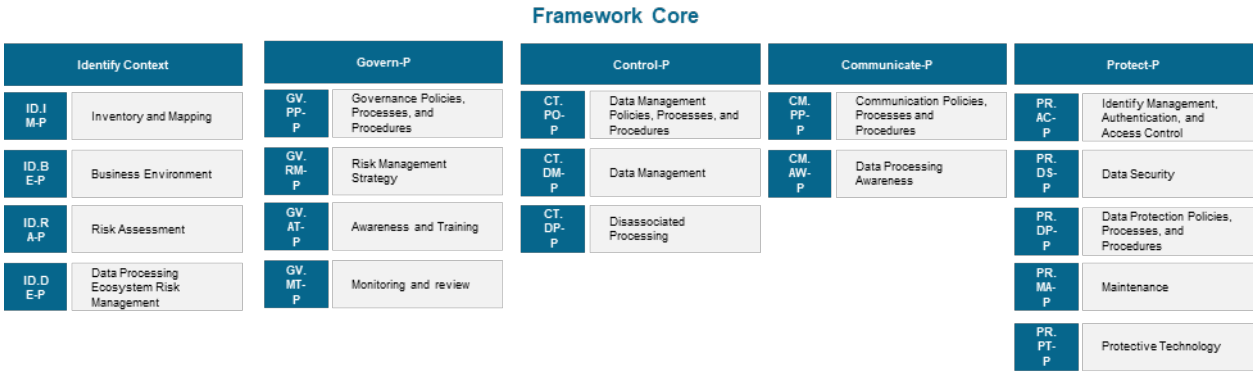

Figure 9 Framework Core categories for the NIST Privacy Management Framework

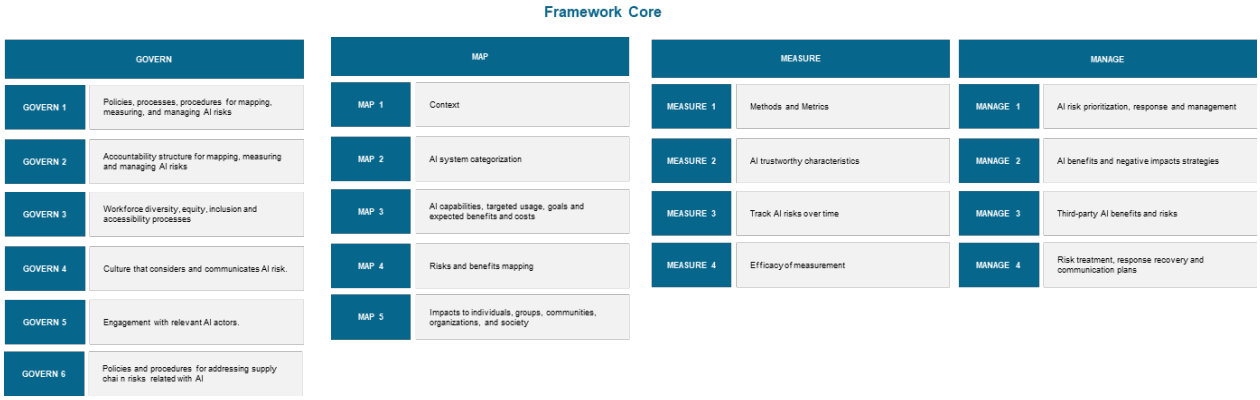

Figure 10 Framework Core categories for the NIST AI Risk Management Framework

3.2 Healthcare Related Risk Management Framework

3.2.1 ISO 14971

ISO 14971 is a risk management standard for manufacturers of medical devices [14] [15]. It describes the process by which manufacturers can manage the risks of their MD throughout its life cycle. It outlines how to structure the risk management process and what activities should be performed to guarantee MD safety for medical use.

According to the International Organization for Standardization (ISO), the European standard EN ISO 14971:2019, together with amendment A11:2021, Annexes Z addresses the coverage of the MDR and IVDR regulations by the standard [14], [16].

Funded by Horizon Europe Framework Programme of the European Union

Risk Management process described in ISO 14971 and depicted in Figure 11 has six stages:

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

Funded by Horizon Europe Framework Programme of the European Union

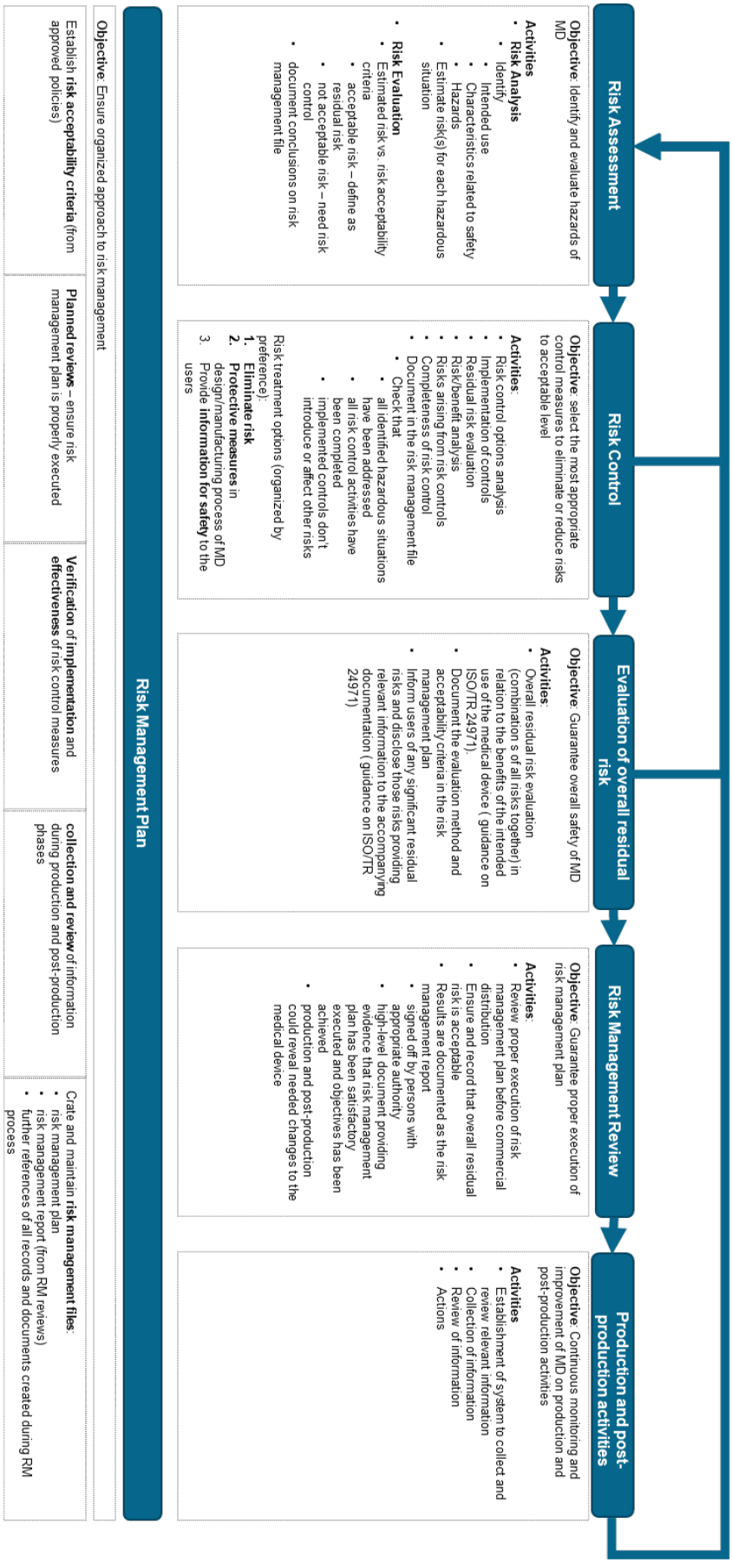

Figure 11 ISO 14971 Risk management process

Funded by Horizon Europe Framework Programme of the European Union

Risk Management Plan

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

Risk Assessment

The risk assessment stage has two sets of activities: risk analysis and risk evaluation. In the risk analysis activities, the intended use of the MD, safety characteristics and hazards are identified. Intended use refers to the objectives which the DM was designed to fulfill by the manufacturer. Safety characteristics refers to any characteristic of the MD that can affect the safety of the device. A hazard is a potential source of harm. For more information on the classification of the medical device use classification, please refer to Figure 12, [14] and [17]. Then, risks are estimated for each hazardous situation. In the risk evaluation activities, each identified risk is evaluated against the risk acceptability criteria defined in the risk management plan stage. Acceptable risks are deemed residual risk and the risks that are not acceptable will need risk control measures. All the risk assessment process activities, methodologies used and results should be documented in the risk management file.

Risk Control

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

The risk treatment options follow a hierarchy of preferences:

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

The selected controls must be implemented, and a new risk assessment must be performed. (see Figure 11). The process of risk analysis and risk control measures implementation goes on as long as there are still risks that are not acceptable and there exists control measures that can be implemented. Once we arrive at a stage where there are still risks with no practical controls to be implemented, the manufacturer has three options: perform a risk-benefit analysis, restrict the intended use or modify the medical device [14]. Otherwise, the MD should not be further developed and commercialized.

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

Evaluation of overall residual risk

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

Funded by Horizon Europe Framework Programme of the European Union

Risk Management Review

The Risk Management Review stage concerns with controlling the proper execution of the risk management plan before commercial distribution of the MD. It guarantees that all records concerning residual risks exists, are properly performed and that every residual risk is acceptable. These controls are done in the form of reviews and they are documented in risk management reports which obliges the clearance/acceptance of a person with the due authority within the manufacturer's organization.

Production and Post-Production Activities

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

Funded by Horizon Europe Framework Programme of the European Union

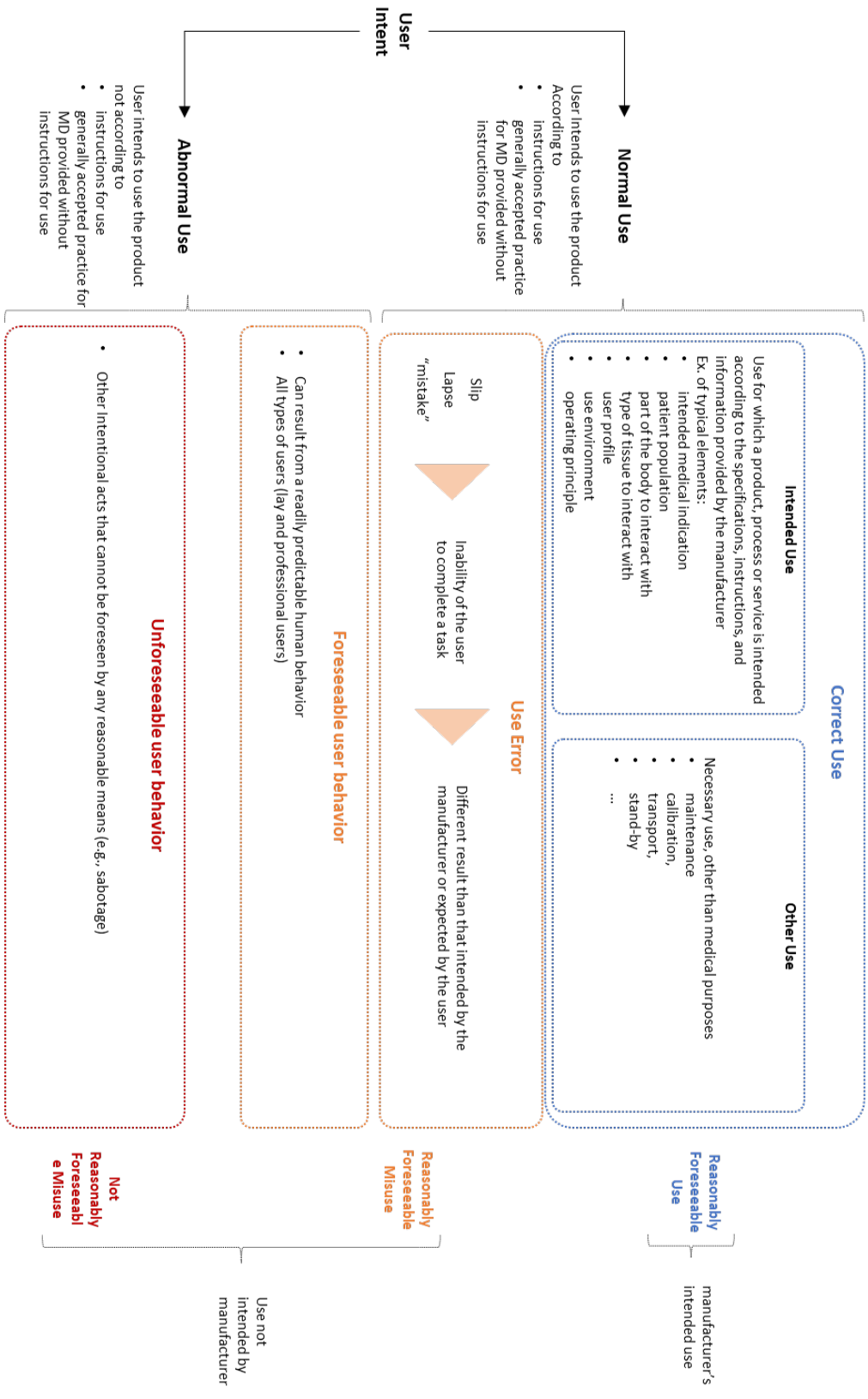

Figure 12 Relation between use and misuse medical device adapted from [14] and [17]

Funded by Horizon Europe Framework Programme of the European Union

3.3 Country Standards

3.3.1 Germany

In Germany, the Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security, abbreviated as BSI), is the entity responsible for publishing the standards regarding information security.

IT-Grundschutz, the BSI methodology for information security, delivers guidelines for the implementation of an information security system. It is designed in a modular and holistic way, so that it's easily adapted to various deployment environments, for any type and size of organziation [18]. IT-Grundschutz is continuously updated and improved by BSI.

The IT-Grundschutz is composed by the following documents:

- IT Grundschutz Compendium;
- BSI Standard 200-1 - Information Security Management Systems (ISMS);
- BSI Standard 200-2 - IT-Grundschutz Methodology;
- BSI Standard 200-3 - Risk Analysis based on IT-Grundschutz;
- BSI Standard 200-4 - Business Continuity Management;

The IT-Grundschutz compendium contains process and system modules for typical business processes, applications, systems, communication connections, and rooms [18]. It covers areas that may be found in organisations, namely:

- Organization and personnel
- IT operations
- Production and manufacture using Industrial Control Systems (ICS),
- Components from the IoT field.

The process oriented modules are:

- ISMS (Information Security Management System);
- ORP (Organisation and Personnel);
- CON (Concepts);
- OPS (Operations);
- DER (Detection and Reaction).

The System-Oriented Module are:

- IND (Industrial IT);
- APP (Applications);
- SYS (IT System);
- NET (Networks and Communication);
- INF (Infrastructure).
- These modules are adaptable to the organisation's own requirements and needs [18].

The 200-1 Information Security Management System (ISMS) defines the requirements for an ISMS and it is compatible with ISO/IEC 27001 [18]. This document "describes, in a step-by-step fashion, how successful information security management may be established and which tasks the management level in government agencies and companies will have in this context" [18].

The 200-2 IT-Grundschutz methodology provides different methodologies, depending on the security level objectives, with information regarding how to operate an ISMS in practice, including [18]:

Funded by Horizon Europe Framework Programme of the European Union

- Information security tasks;
- Design of organizational structure for information security;
- How security policy can be developed in practice;
- How appropriate security requirements can be selected;
- What should be considered when implementing the security policy;
- How to maintain and improve information security during routine operation.

IT-Grunschutz methodology follows the ISO standards 27001 and 27002 [18], [19].

The 200-3 - Risk analysis on the basis of IT-Grundschutz document describes a risk analysis methodology, based on the threats described in the IT-Grundschutz compendium [18], [20].

100-4 Business Continuity Management describes the methodology for establishing and maintaining an organization-wide business continuity management [18] and it complements the BS standard 200-2 [18].

3.3.2 Italy

The Italian National Cybersecurity Framework, called “Framework Nazionale per la Cybersecurity e la Data Protection”, follows closely the NIST Cybersecurity Framework described in section 3.1.3, which does not include any control mechanism for adhering to the GDPR.

In essence the Italian framework is composed of the same three components as the NIST CSF:

- The **network Core**, which organizes activities for ongoing cyber risk management. They are organized in 5 categories: Identify; Protect; Detect; Respond and Recover. Each category contains subcategories with specific activities/controls.
- The **Framework Profiles**, which result from the selection of the needed Framework Core activities, according to the business objectives of the organization, the threat environment and the determined requirements.
- The **Implementation Tiers**, which specifies the maturity of the cybersecurity risk management framework.

Unlike the NIST CSF, new controls were added to the network core in order to cover GDPR regulation for data protection. They added seven subcategories in the Identify category and one subcategory in the Response category.

The Identify category was complemented with controls related to

- Roles and responsibilities related to personal data processing and protection are defined and made known to everyone in the organization and relevant third parties (e.g., suppliers, customers, partners);
- Identification and documentation of Personal data processes;
- Data Protection Impact Assessment;
- Definition, implementation and documenting of subject's information processing activities;
- Definition, implementation and documenting Processes for collecting and revoking data processing consents;
- Definition, implementation and documenting of subjects rights (e.g, right to access, rectify, cancel, etc.);
- Definition, implementation and documenting data transfer processes in the international context.

Funded by Horizon Europe Framework Programme of the European Union

The Response category was complemented with controls for personal data violation incidents, where the organization following the framework must document these incidents and, if necessary, the subject and relevant authorities are informed.

3.3.3 Spain

The Spanish National Security Framework, Esquema Nacional de Seguridad (ENS), is regulated by the Royal Decree named “Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad” [21].

This document presents the **Basic Principles** to consider when dealing with information security:

- Security as an integral process,
- Risk-based security management,
- Prevention, detection, response and conservation,
- Existence of lines of defense (protection strategy consisting of multiple layers of security),
- Continuous monitoring and periodic re-evaluation
- Differentiation of responsibilities.

Then it provides guidelines and obligations for the security risk management and analysis in general. It provides security requirements on

- the risk management process, policies;
- Guidance on Information Systems Categorization;
- Human Resources and competences;
- Access control;
- Facilities protection;
- product and services procurement;
- contracts;
- system integrity;
- System updates;
- data and communication protection;
- audit logs;
- security incidents;
- business continuity;
- continual improvements of the security process;
- Audit, report and Security Incident response;
- Determination of minimum security requirements;
- Guidance on Information Systems Categorization.

The ENS is compatible with ISO 27001 as indicated in the “CCN-STIC 825 ENS – Certifications 27001” [22] and “Independent Annex – mapping ISO 27001:2022 and RD 311/2022” [23] documents published by the Spanish National Cryptology Centre.

Funded by Horizon Europe Framework Programme of the European Union

4 Emerging Technologies

In this section, the emergent technologies challenges and requirements elicited during CYLCOMED partners' interviews summarized. The Emergent technologies are the following:

- Internet of things;
- Cloud services;
- Artificial Intelligence;
- 5G network and services;
- Blockchain.

4.1 Internet of Things

According to [24], IoT is defined as "an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and interact."

Smart watches and body sensors can be regarded as IoT devices. Even other more complex systems such as infusion pumps can be connected to the Internet and function as an IoT device. IoT devices have potential for enhancing the way healthcare services are provided. For example, remote monitoring of patient's condition while at home.

On the other hand, IoT devices come with a new set of vulnerabilities not considered until now or certain services. IoT top 10 vulnerabilities described by the OWASP organization are the following [25]:

- Weak, guessable or hardcoded passwords;
- Insecure Network Services;
- Insecure Ecosystem Interfaces;
- Lack of Secure Update Mechanism;
- Use of Insecure or Outdated Components;
- Insufficient Privacy Protection;
- Insecure Data Transfer and Storage;
- Lack of Device Management;
- Insecure Default Settings;
- Lack of Physical Hardening.

When interviewing the CYLCOMED partners, aside from the OWASP top 10 vulnerabilities, the following challenges/concerns for IoT devices were the following:

- The quality of data;
- The formats of the data;
- IoT devices use open source systems which have lack of testing on new versions of applications.

During the interviews, the following recommendations/requirements was indicated:

- Consider intended use and criticality of medical device when designing it;
- Processes, procedures and tools for guaranteeing accuracy of information must be in place;
- Processes, procedures and tools for guaranteeing accuracy of information Audit logs must be in place;
- The information security priorities should have a hierarchy that prioritizes patient safety. Integrity should have the highest priority to avoid any type of risk or hazard during medical act. Then, Availability should have the next highest priority since it can stop

Funded by Horizon Europe Framework Programme of the European Union

procedures and have an impact on patient's safety. Third comes confidentiality which poses no safety risk for medical act, but is important for legal compliance. Note that confidentiality is still important, but it's not critical when it comes to patient's safety.

- Use FMEDA Methodology – Failure modes, Effects, Diagnosis Analysis – for analyzing medical device.

4.2 Artificial Intelligence

According to the ISO/IEC Joint Technical Committee (JTC) 1, Artificial Intelligence refers to "an interdisciplinary field, usually regarded as a branch of computer science, dealing with models and systems for the performance of functions generally associated with human intelligence, such as reasoning and learning" [26].

Artificial Intelligence has several promising use cases in healthcare, including diagnosis assistance, nursing and managerial assistance, precision and genomic medicine, among others [27], [28].

According to an European Parliament published document [29], the risks of AI in healthcare are the following:

- Patient harm due to AI errors;
- Misuse of medical AI tools;
- Risk of bias in medical AI and perpetuation of inequities;
- Lack of transparency;
- Privacy and security issues;
- Gaps in AI accountability;
- Obstacles to implementation in real-world healthcare.

During our interviews, the following challenges for AI technologies emerged:

- When using the AI system, it is not clear with whom the responsibilities lie. For example, who is responsible, the clinician or the AI system when it is used for drug development/drug dosage determination or if a patient dies as a result of an AI driven decision/action?
- AI systems are hard to validate. Validation process involves proving that some system is working properly. It is crucial to demonstrate that the operations, project development, risk analysis, implemented risk controls, test, etc. followed adequate procedures. This means that it must be adequately documented. Then, the auditors have to review and to have a high level of expertise, be well trained and cover a wide range of different areas. And it is hard to establish the number of patients in the validation process, so that the validation is correct and that guarantees that the application is secure.
- AI systems might exhibit limited generalization capabilities, which becomes particularly concerning in critical healtcare applications. New unseen situations for which the AI system was not explicitly trained, could potentially harm patient health.
- The concept of adversarial attacks, in which slight changes to patient data (medical images, reports or clinical measurements) could cause an AI model to produce false results, is particularly concerning in the context of cybersecurity.
- Guaranteeing data quality and integrity is crucial for properly training the AI model.
- How to determine the right AI model?
- Lack of regulation on this technology.
- Wrong diagnosis that can impact human lives.
- How to manage biases on data?
- Data poisoning, which could cause biases or deviation on AI models.

Funded by Horizon Europe Framework Programme of the European Union

The following requirement/recommendations were indicated by the interviewees:

- Medical staff should use AI system as consultant, to confirm or facilitate medical decision. Medical staff should not be entirely confident of the AI system.
- There must be processes and procedures to teach data providers to think and look to data in the right way, so that data quality is improved.
- The providers must anonymize data whenever is legally required.
- Selection of AI model should follow a formal test and development lifecycle and should be done by experts on the field to rely on their experience.
- The solution provider should give support for incident response and integration with other systems.
- In order to control data poisoning and biases on data, the solution provider should use representative training data and implement additional techniques such as data augmentation approaches, generation of synthetic data using generative models or any other adequate solution.

4.3 Cloud Technology

According to NIST, cloud computing is a “model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [30].

Cloud solutions can be used for electronic health records, medical imaging, telemedicine, patient monitoring, among other use cases [31].

According to OWASP, the cloud top 10 vulnerabilities are the following [32], [33]:

- Account and Data Ownership;
- User Identity Federation;
- Regulatory Compliance;
- Business Continuity and Resiliency;
- User Privacy and Secondary Usage of Data;
- Service and Data Integration;
- Multi-Tenancy and Physical Security;
- Incidence Analysis and Forensic Support;
- Cloud Infrastructure Security;
- Non-Production Environment Exposure.

During our interviews, the following challenges for Cloud technologies emerged:

- Business continuity challenges resulted from the premise control loss.
- Ownership of data.
- Secondary use of data, as medical data could be very profitable for the cloud service provider.
- Cloud service providers are more experienced with cybersecurity/incidents as they deal with more cases/clients/technologies/attackers.
- There might be regulatory constrains regarding the use of public cloud services in the healthcare setting.
- The lack of data sources organization leads to data warehousing problems.

The following requirement/recommendations were indicated by the interviewees:

- Intended/final use of cloud services should be considered in the risk analysis process to determine what is safe and what is not. For critical service for operational

Funded by Horizon Europe Framework Programme of the European Union

performance in hospitals, this type of services should not used. For not so critical services, the risks must be clearly evaluated.

- The Cloud security Alliance controls and European Commission cloud guidelines must be followed.
- Whenever feasible, use cloud infrastructure that is local or geographically close to the organization.
- When exporting data from organization site, use highest encryption key possible.
- Rules and access controls to deny unauthorized accesses or operations of the data on cloud services must be implemented.
- Cloud provider should follow/implement recognized standards (for example, ISO 27001 and other specific and relevant to use cases).
- Cloud services usage must be evaluated for individual use cases by use case and it should include a comparative evaluation between using cloud services providers and hospitals private clouds.

4.4 5G networks and Services

5G is the 5th generation of mobile technologies. The ITU-R defined the three main usage scenarios [34]:

- **"Enhanced Mobile Broadband (eMBB)**, which deals with increased data rates, high user density and very high traffic capacity for hotspot scenarios, as well as seamless coverage and high mobility scenarios with still improved used data rates."
- **"Massive Machine-type Communication (mMTC)** for the IoT, requiring low power consumption and low data rates for very large numbers of connected devices."
- **"Ultra-reliable and Low Latency Communications (URLLC)** to cater for safety-critical and mission critical applications."

With the three main usage scenarios, 5G could enable remote surgery, remote healthcare based on virtual reality (VR) and augmented reality (AR), Massive Internet of Medical Things (IoMT) for tracking patient's status [34], [35].

The American Telephone and Telegraph organization (AT&T) describes security concerns from increased attack surfaces that 5G network brings with all the new technologies that it needs to deploy [36]:

- Large attack surface due to the massive increase in connectivity;
- Greater number of devices accessing the network;
- IoT: Extension of security policy to new types of devices;
- Authentication of a larger number and wider variety of devices;
- Insufficiency of perimeter defenses;
- Unknown security vulnerabilities with 5G AKA (Authorization and key Agreement);
- Automated change to the network;
- Ephemeral nature of workloads, including dynamic bursting/scaling;
- Uncertainty about the physical locations of workloads;
- The need to secure Multi-access Edge Computing (MEC);
- Enables the movement and access to higher quantities of data;
- It's an immature and untested set of technologies;
- Depend on 5G for more mission-critical apps;
- Many use cases and threats are still unknown.

Funded by Horizon Europe Framework Programme of the European Union

During our interviews, the following challenges for 5G networks emerged:

- For critical applications can be very dangerous;
- Continuity of connection could be very problematic, especially if patient's life depends on it;
- Lagging of connection could endanger patients' life in critical use cases like remote surgery;
- Inconsistency of 5G networks – it doesn't work everywhere in the same way;
- Too much unknowns for critical use cases like remote surgery;
- It's not clear how to leverage new devices in trusted environment;
- 5G, being projected to be a virtualized infrastructure with AI powered orchestration, will need a SIEM system to perform infrastructure monitoring. If an attack happens to the infrastructure, the 5G service provider will be overloaded with SIEM system because SIEM systems are based on indexing. This is a big data problem.
- Not clear how to manage flexibility of 5G network with critical applications.
- Throughput could be unstable for several reasons (5G network is very complex).

The following requirement/recommendations were indicated by the interviewees:

- Critical medical (surgical) interventions, monitoring or treatment should preferably not be administered or performed over 5G connection. Exceptions could include following scenarios:
    - For dealing with a patient with a dangerous and contagious disease;
    - If the surgery requires very rare skills and only if there are more surgeons/medical staff in the room for assistance.
- 5G should improve or maintain, but not impair current services/medical actions;
- Use of 5G should be evaluated use case by use case;
- Robots functioning with remote commands should have built-in capabilities for safe functioning in case of connection losses;
- Evaluate use case by use case, for example, the need for high amount of data and the update frequency of devices data being sent to hospitals.

4.5 Blockchain

According to NIST, a blockchain is "a distributed digital ledger of cryptographically-signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules" [37].

Some potential use cases for blockchain in healthcare can be found in [38] and they are:

- Prescription tracking to detect opioid overdose and over-perscription;
- Data sharing to incorporate telemedicine with traditional care;
- Sharing cancer data with providers using patient-authorized access;
- Cancer registry sharing to aggregate observations in cancer cases;
- Patient digital identity management for better patient record matching;
- Personal health records for accessing and controlling complete health history;
- Health insurance claim adjudication automation to surface error and fraud.

There exists several blockchain technologies that serve a multitude of purposes. In [39] the blockchain vulnerabilities were organized for different blockchain technologies (see Figure 13).

Funded by Horizon Europe Framework Programme of the European Union

Figure 13 Blockchain vulnerabilities organized by the most known blockchain technologies. Image based on [39].

Funded by Horizon Europe Framework Programme of the European Union

During our interviews, the following challenges for blockchain technology emerged:

- Blockchain technologies are difficult to implement in real-life scenarios because it might require complete change on the workflows inside the hospitals. It might require creation of infrastructure, proper devices/applications for medical staff to use the blockchain and procedures would have to change. Moreover, in the legal point of view, how do we deal with something that goes wrong with smart contracts?
- If organizations use different types of blockchain technologies, making them compatible among organizations might take years.
- Difficulties of processing data from different sources with no legal or technical problems.
- Governance issues will emerge since blockchain is supposed to work in a distributed, peer-to-peer network in order to fulfill its potentials.
- Energy consumption and latency due to consensus mechanism are well-known issues for blockchain technologies.
- There is no clear vision on how to solve problems when there are bugs on smart contracts. This is a governance problem.
- Blockchain is very slow for searching (blockchain vs. analytics).

The following requirement/recommendations were indicated by the interviewees:

- Use hashes and off-chain databases to manage data confidentiality;
- Be ready to use quantum resistant cryptography;
- The use of blockchain technologies must follow standards (e.g., GAIA-X, IDSA).

Funded by Horizon Europe Framework Programme of the European Union

Conclusions

This deliverable is part of an ongoing process of risk management framework analysis, elicitation of emergent technologies requirements and design of a risk management framework for connected medical devices.

In this report, the risk management frameworks described in the chapters reflects a part of a bigger analysis performed in the survey done on risk management frameworks. In essence, all the analyzed risk management frameworks have the following characteristics:

- Requires the definition of the scope and context;
- Governance structure to guarantee the implementation and operation of the risk management process;
- Allocation of resources (human resource and technologies);
- Risk analysis and controls selection;
- Monitoring and review of the implemented controls;
- Record keeping for all the risk management activities;
- Continuous monitoring of the risk management process.

From the requirements elicitation for Emergent Technologies, we can generally conclude that the intended use of the technologies and criticality for patient safety must be considered. Data quality and integrity is crucial for avoiding risks or hazards during medical act (e.g., due to wrong diagnosis). Availability of systems play a crucial role as well, since without the adequate resources, patients cannot be treated properly. Following standards and best practices are crucial for guaranteeing a minimal level of security and safety. Other technology specific requirements were drawn as well.

The Emergent technologies requirements elicited until now is also a part of an ongoing process. More interviews will be performed with the CYLCOMED partners as the project evolves. The process of risk management frameworks surveying and partners' interviews will continue as the CMD risk management framework is designed.

The next steps for developing the CYLCOMED risk management framework are the following:

- The emergent technologies challenges will be further analyzed to determine more requirements, recurring to desk research and new methodologies and tools to tackle those challenges;
- Design of a first version of the CYLCOMED risk management framework based on the analyzed requirements and risk management methodologies;
- Continuous update on risk management frameworks and related documents;
- New set of meetings with the CYLCOMED partners for enhancing the preliminary CYLCOMED risk management framework.

Funded by Horizon Europe Framework Programme of the European Union

References

[1] Portuguese National Cybersecurity Centre, «National Cybersecuity Framework,» Portuguese National Cybersecurity Centre, 2020.

[2] 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,» chez *3rd International Conference on Management, Economics and Finance*, Amsterdam, 2021.

[3] Institute of Risk Management, «A Risk Practitioners Guide to ISO 31000:2018,» Institute of Risk Management.

[4] Australian Government Comcover, «An Overview of the Risk Management Process,» Australian Government Comcover.

[5] Internantional Organization for Standardization, «ISO/IEC 27000 family,» [En ligne]. Available: https://www.iso.org/standard/iso-iec-27000-family. [Accès le November 2023].

[6] Internation Organization for Standardization and International Electrotechnical Comission, ISO/IEC 27001:2022 - Information Security Management System.

[7] 2001 Acacemy, «Clause-by-clause explanation of ISO 27001 White Paper,» 2001 Acacemy, 2016.

[8] Zoé Hoy and Andrea Foley, «A structured approach to integrating audits to create organisational efficienties: ISO 9001 and ISO 27001,» *Total Quality Management & Business Excellence.*

[9] isms.online, «ISO 27001:2022 Annex A Explained - Complete Guide,» [En ligne]. Available: https://www.isms.online/iso-27001/annex-a/. [Accès le November 2023].

[10] Svetlana Kim, «ISMS Implementation and Maintenance in Compliance with Finland's National Cybersecurity Requirements, Bachelor's Thesis,» Haaga-Helia University of Applied Sciences.

[11] National Institute for Standards and Technology, [En ligne]. Available: https://www.nist.gov/system/files/documents/pml/div683/conference/May_final.pdf.

[12] National Institute for Standards and Technology, [En ligne]. Available: https://www.nist.gov/cybersecurity.

[13] National Institute of Standards and Technology, «NIST Cybersecurity Framework,» [En ligne]. Available: https://www.nist.gov/cyberframework. [Accès le November 2023].

Funded by Horizon Europe Framework Programme of the European Union

[14] British Standards Institution (BSI), «Risk management for medical devices and the new BS EN ISO 14971,» British Standards Institution (BSI).

[15] Stephen G. Odaibo, «Risk Management of AI/ML Software as a Medical Device (SaMD): On ISO 14971 and Related Standards and Guidances,» *ArXiv,* n° %1abs/2109.07905, 2021.

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

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

[18] Bundesamt fur Sicherheit in der Informationstechnik, «BSI-Standard 2001 - Information Security Management System (ISMS),» Bundesamt fur Sicherheit in der Informationstechnik, 2017.

[19] Bundesamt für Scherheit in der Informationstechnik, «BSI-Standard 200-2 - IT-Grundschutz Methodology,» Bundesamt für Scherheit in der Informationstechnik, 2017.

[20] Bundesamt für Sicherheit in der Informationstechnik, «BSI-Standard 200-3 Risk Analysis based on IT-Grundschutz,» Bundesamt für Sicherheit in der Informationstechnik, 2017.

[21] Ministerio de Assuntos Económicos y transformación Digital, «Royal Decree 311/2022 of 3 May regulating the National Security Framework,» Ministerio de Assuntos Económicos y transformación Digital, 2022.

[22] C. C. Nacional, «ICT Security Guide CCN-STIC 825 National Security Framework. 27001 Certifications,» Centro Criptológico Nacional, 2023.

[23] N. C. Centre, «ICT Security Guide CCN-STIC 825 Independent Annex Mapping between the ISO27001:2022 Standard and the RD 311/2022(ENS),» National Cryptology Centre.

[24] ISO/IEC JCT1, «Internet of Things (IoT) Preliminary Report,» 2014.

[25] [En ligne]. Available: https://owasp.org/www-chapter-toronto/assets/slides/2019-12-11-OWASP-IoT-Top-10---Introduction-and-Root-Causes.pdf.

[26] International Electrotechnical Commission, «Atificial Intelligence across industries,» International Electrotechnical Commission, 2018.

[27] DonHee Lee and Seong No Yoon, «Application of Artificial Intelligence-Based Technologies in the Healthcare Industry: Opportunities and Challenges,» *International Journal of Environmental Research and Public Health,* 2021.

Funded by Horizon Europe Framework Programme of the European Union

[28] Sameer Quazi, «Artificial intelligence and machine learning in precision and genomic medicine,» *Medical Oncology,* vol. 39, n° %1120, 2022.

[29] European Parliamentary Research Service, «Atificial Intelligence in Healthcare Applications risks, and ethical and societal impacts».

[30] National Institute of Standards and Technology, «The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology,» National Institute of Standards and Technology.

[31] Deloitte, «Improving patient health and care with cloud solutions - cloud technology for health care and life sciences,» [En ligne]. Available: https://www2.deloitte.com/us/en/pages/consulting/articles/healthcare-cloud-solutions.html. [Accès le 11 2023].

[32] [En ligne]. Available: https://hitachi-systems-security.com/the-top-10-owasp-cloud-security-risks/. [Accès le November 2023].

[33] [En ligne]. Available: https://owasp.org/www-pdf-archive/OWASP_Cloud_Top_10.pdf. [Accès le November 2023].

[34] European Telecommunications Standards Institute, [En ligne]. Available: https://www.etsi.org/technologies/5g. [Accès le 11 2023].

[35] Dumitrel Loghin et. al., «The Disruptions of 5G on Data-Driven Technlogies and Applications,» *IEEE Transactions on Knowledge and Data Engineering,* vol. 32, n° %16, 2020.

[36] American Telephone and Telegraph, «AT&T Cybersecurity Insights™ Report: Security at the Speed of 5G,» [En ligne]. Available: https://cybersecurity.att.com/blogs/security-essentials/att-cybersecurity-insights-report-security-at-the-speed-of-5g. [Accès le 11 2023].

[37] National Insititute of Standards and Technology, «Developing Cyber-Resilient Systems: A Systems Security Engineering Approach,» 2021.

[38] Peng Zhang, Douglas C. Schmidt, Jules White, Gunther Lenz, «Chapter One - Blockchain Technology Use Cases in Healthcare,,» chez *dvances in Computers, Volume 111*, Elsevier, 2018, pp. 1-41.

[39] Huru Hasanova, Ui-Jun Baek, Mu-gon Shin, Kyumghee Cho and Myung-Sup Kim, «A survey on blockchain cybersecurity vulnerabilities and possible countermeasures,» *International Journal of Network Management,* vol. 29, n° %12, 2019.

[40] F. D. a. K. Nordström, «A Comparative Analysis of Industrial Cybersecurity Standards,» *IEEE Access,* vol. 11, n° %110.1109/ACCESS.2023.3303205, pp. 85315-85332, 2023.

Funded by Horizon Europe Framework Programme of the European Union

Funded by Horizon Europe Framework Programme of the European Union