Digital Europe Programme

(DIGITAL)

Project HISC4ALL

Health Information Safe and Cybersecured for All

Second Project Report

Version 2.0

31 December 2023

Table of Contents

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

1. Project Information

Project Information	
Project Name	Health Information Safe and Cybersecure for All (HISC4ALL)
Project Code	101100701 – HISC4ALL – DIGITAL-2022-CYBER-02
Reporting Period	Phase II / WP2, started in May 2023 and ended in December 2023
Report Date	5th January 2024
Project Manager	Alberto Lima Caria (Paldata)
Project Sponsor	Paulo Marques Pinto (INEM)

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

2. Project Overview

2.1 The elements of a consortium

Consortium Composition in the Agreement date

The Consortium was composed in the beginning by the following organizations, INEM and Pahldata, focused in the healthcare sector. The consortium mobilizes a very experienced multidisciplinary team with synergetic and complementary activities in Consulting, Researching and Investigation. The partners involved have extensive clinical, information security cybersecurity and business experience to enrich the present project.

Considering that the scope of this project is reasonably wide, the Consortium includes the INEM and Pahldata, a consulting firm specialized in the health sector with considerable experience in cybersecurity.

Consortium inclusion of a new member with an Amendment document

Considering that the original application consisted of three organisations INEM; Pahldata and others, after submission it was realised that the third organisation could not be part of the consortium due to EU regulations. The consortium was therefore formed with two organisations (INEM + Pahldata), with the aim of the inclusion of a third organisation as soon as possible.

This was done in June 2023, with the request of inclusion of the Centro Hospitalar Universitário de São João, Porto (CHUSJ), process already concluded.

Each member is presented in detail below.

INEM (www.inem.pt) – is the National Institute for Medical Emergency, responsible for coordinating the operation of an Integrated System for Medical Emergency that guarantees the emergency and adequate provision of healthcare to victims of a casualty or sudden illness.

The main tasks of INEM are the provision of medical emergency care at the location of the occurrence, the assisted transport of victims to the hospital, and the coordination between the various stakeholders of the System: Police (through the European emergency number – 112), central entities of the Ministry for Health, Public Hospitals, Private Hospitals, Firefighters, among others.

INEM mission is to ensure the effective functioning and sustainable development of the Integrated Medical Emergency System (IMES). Its vision is to be an innovative, sustainable, and reference organization in the provision of out-of-hospital emergency medical care, assuming itself as a brand of excellence in the health sector and its values are:

- Ambition;
- Humanism;
- Innovation;

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

- Ethics;
- Competence;
- Efficiency;
- Responsibility.

To ensure the fulfilment of its attributions, INEM provides the following set of services organized on areas of activity/intervention:

- The activity of the Urgent Patient Guidance Centres (UPGC - Portuguese CODU), working 24 hours a day, 365 days a year;
- Righter pre-hospital care for victims of an accident or sudden illness, working 24 hours a day, 365 days a year, providing emergency medical care in a pre-hospital environment, and providing transport to the appropriate health facilities;
- Regulation of Automated External Defibrillation (AED) activity in an out-of-hospital environment and implementation of a National AED Program (PNDAE in portuguese);
- Licensing the activity of transporting patients and vehicles assigned to it through licenses and audit services;
- Planning, coordination, and provision of medical assistance;
- Training and promotion of the training of professionals essential to medical emergency actions;
- Training and promotion of training for the general public;
- Accreditation of external entities for training in Medical Emergency;
- Dissemination of INEM activities.

CHUSJ (https://portal-chsj.min-saude.pt/) – Centro Hospitalar Universitário de São João, Porto - www.portal-chsj.min-saude.pt – is a public Public sector hospital, integrated in the Portuguese public health system, reporting to the Ministry of Health, located in the city of Porto and provides direct assistance to the population of the municipality of Porto, as well as the municipalities of Maia and Valongo, also acting as a reference center for the districts of Porto, Braga and Viana do Castelo, in the north of Portugal. The CHUSJ also acts as a reference for wider geographic areas, in the context of Hospital Referral Networks, or even for wider areas in specific areas.

CHUSJ management activity is structured at intermediate management levels. Intermediate management structures bring together services (which can be organized into functional units) and organic units that, in an articulated manner, contribute to the pursuit of established objectives. Organic units are simpler structures than services, with specific functions, equipped with their own human and/or technical resources, not integrated into services:

- **Clinical Production Areas:** Surgery; Medicine; Emergency and Intensive Medicine; Psychiatry and Mental Health; Complementary means of diagnosis and therapy; Woman and Child.
- **Clinical Production Support Areas:** Hospital Epidemiology; Outpatient clinic; Clinical Trials;
- **Support Areas:** Management and Information Center; Humanization Service.

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

Pahldata (name updated to Paldata) (www.pahldata.pt) – is a medium organization (SME) of the IT sector created in 1987 developing activities for the Healthcare, Defence, Banking, Telcos, Manufacturing, Energy, Transports, and Public sectors, with 48 collaborators. Paldata has a participation in Quattro (Healthcare company), which is a Healthcare Information Solutions Provider, with a mission to leverage digital transformation in the healthcare sector. Both companies provide value-added solutions to the Portuguese and international health sector that address current and future challenges. There qualified teams are committed to understanding the challenges and problems of customers and therefore seeking innovative and disruptive solutions that provide value, materialized in effectiveness and efficiency.

The need to address the trends and demands of the Healthcare sector, with undergoing great pressure, dynamism, and digital evolution, led to the identification of the following offer of solutions and services, in the main areas of intervention:

- Information and Communications Technology;
- NOC – Network Operations Center;
- SOC – Security Operations Center;
- Smart Health;
- Software & Consulting

2.2 Role and Activities to Develop in HISC4ALL

The main reason for the participation of a hospital as a beneficiary element of the project is from the outset related to the use cases, as well as the orientation to other stakeholders of the results to be achieved with the project:

Target Stakeholders of the project

- Hospitals;
- Health Clinics;
- Institutions for the Public National Health Service (NHS);
- SMEs for the healthcare sector (small hospitals, clinics, dentists, pharmacies);
- Non-profit organizations (Firefighters).

Therefore, the participation of a Hospital in the Project will bring the following benefits and added value to the project activities & results:

- ✓ Be a participant and simultaneously a beneficiary of the framework and application to be developed in the project;
- ✓ Bring an informed and experienced in health sector orientation to the project;
- ✓ Contribute to and validate the set of activities and deliverables resulting from the different phases;

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

- ✓ To participate in the pilot of Proof-of-Concept (POC) and in the communication and dissemination activities, in order to ensure the visibility of the project for the healthcare eco-system and community.

Use Cases Characterisation

Objectives for the Framework

(1) **Use Case INEM:** Protect the flows and the bubble of applications and clinical information installed, generated and processed between sites and on each mobile unit;

(2) **Use Case Medical Equipment**: To improve the security of medical devices, as well as the functional and technical protocols used, in terms of storage, processing and transmission of information, with users and other systems or devices;

(3) **Use Case Shared:** To guarantee and grant confidence to workflows, standardising with security the existing interfaces between the different entities that intend to share information, ensuring compatibility in the maturity levels of security between entities, through the definition of baselines and transition models to be followed, identified by the Framework and Application of the HISC4All project.

Use Case I (INEM): Ensure the Information Security and Cybersecurity of the functional and technical flows, based on applications and devices, in which clinical information is stored, processed or transmitted, as well as the systems that directly support their operation.

Use Case II (INEM): Ensuring the information security and cybersecurity of medical devices by monitoring signals, interfaces and the surrounding environment where they are inserted and used.

Use Case III: Ensure the same level of information security and cybersecurity maturity and level of the Systems that share clinical information between different health entities, in order to ensure security properties (e.g. confidentiality, integrity, availability) and the requirements defined and agreed between the parts (e.g., security baseline to be applied, maturity levels of controls, interoperability).

The HISC4ALL project through the *Framework and the Application* Software shall define security levels, control baselines and transition models in the various security dimensions (e.g. organizational, physical, human, technological), for the referenced Use Cases, as well as the transition criteria between the levels and the maturity levels in the security controls associated with each level/baseline.

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

2.3 Project Objectives

The aim of the project is to **design a common and shared Information Security and Cybersecurity Framework for the health sector** in Europe, based on a pilot project (POC – Proof-Of-Concept) in Portugal, and the development of its replication process for other countries and markets.

The final **Framework** will be supported by a web application that will enable organisms to assess their level of maturity in relation to the benchmarks identified by the framework.

In the context of software development, the Web application is a support structure, with several components (e.g., classes, modules), upon which another software project can be organized and developed, with the resulting advantages (e.g., avoiding time, reducing complexity, sharing an identical view of architecture by all stakeholders).

The **creation of a Framework and its application in the sector will be developed in order to allow answering the central question / problem identified**: *How to guarantee confidentiality, integrity, availability and non-repudiation of clinical data / information shared between health entities in order to minimize Information Security and Cybersecurity risks*?

The main use cases to serve as the POC's reference, are associated with the protection against cyberattacks and the security of information across its entire lifecycle. They will be validated by National Institute for Medical Emergency (INEM) and a Public Hospital.

From the central question, **three derived questions** arise that will guide the design of the Framework and later its application process:

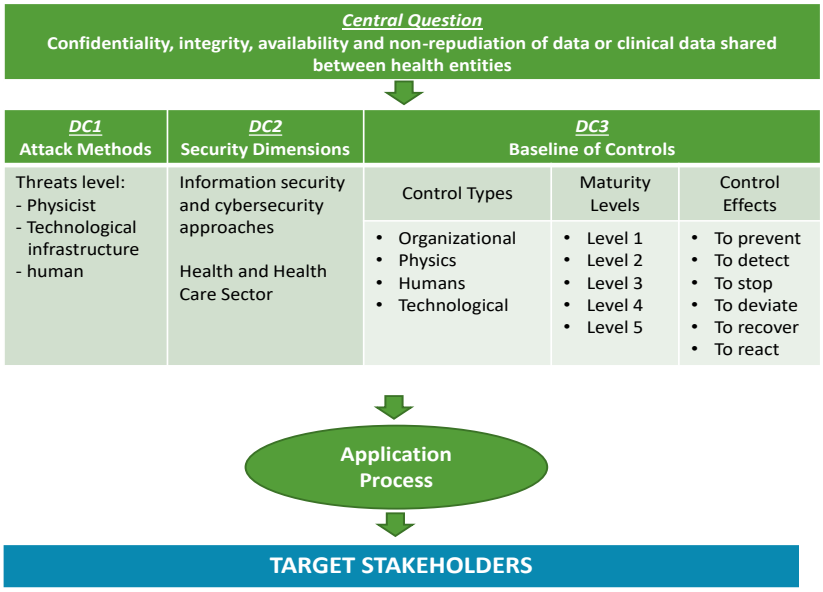
(1) **First derived question (QD1)**: - What are the possible methods of attacking Information Security and Cybersecurity that may occur? The answer to the question will be supported in some of the main taxonomies of attack/threat methods and the identified Use Cases for the System(s).

(2) **Second derived question (QDF2)**: - What are the most relevant dimensions and categories of Information Security and Cybersecurity controls to be implemented? The answer to the question will be supported by a literature review focused on the main general approaches to Information Security and Cybersecurity that exist and, on the specifics, associated with the health sector.

(3) **Third derived question (QDF3)**: - What are the controls baselines to be implemented and the associated control maturity levels? The answer to the question will be supported by the answer to questions one and two and considering the following postulates: (i) the need for different types of controls to be implemented in each baseline (e.g., organizational, physical, human and technological); (ii) existence of five maturity levels for each control (1 to 5); and (iii) effects of controls (e.g. prevent, detect, deter, divert, recover, react and their combination).

The Framework assumes the following configuration:

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."



General Objective from the Scope of the Call

Support cybersecurity resilience in healthcare and health institutions (stress over COVID-19 crisis), in view of limiting the damage of safety-critical cybersecurity incidents which have affected hospitals and health services providers.

- *Develop a common and shared Information Security and Cybersecurity FRAMEWORK for the health sector, and its application process, aiming guarantee confidentiality, integrity, availability and non-repudiation of data or clinical data shared between health entities, in order to minimize the risk of Information Security and Cybersecurity.*

Specific Objectives addressing the Intervention Areas of the Call

- Implementation of objectives and requirements under the NIS Directive in relation to the health sector.
  - *Adopt and implement new products and services that guarantee authenticity and integrity of information, in the context of health institutions or that provide health care, contributing to the objectives and requirements under the NIS Directive in the context of the health sector.*
- Adoption in healthcare and health institutions, and in particular SMEs (Small and Medium Enterprises), of tools, methods, organizational and management practices dedicated to cybersecurity. Also, the exchange of information between peers.
  - *Adopt organizational management methods and practices that contribute to information security and cybersecurity compliance in the SME of the healthcare sector;*
  - *Share Lessons learned resulting from the application of the framework.*
- Cybersecurity education, awareness and skills development in healthcare and health institutions.

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

- *Introduce new training activities in the functioning of framework and in the implementation and operation of the process;*
- *Promote the awareness of the decision makers and users of the sector institutions for information security and cybersecurity;*
- *Promote the implementation of controls associated with information security and cybersecurity in the healthcare sector.*

2.4 Initial Work Packages

The Project has been conceived and implemented through the development of 4 WORK PACKAGES, referring to the four phases of the Project:

- Work Package 1 – DESIGN
- Work Package 2 – MARKET TEST
- Work Package 3 – CONCEPTION & APLICATION
- Work Package 4 – DISSEMINATION

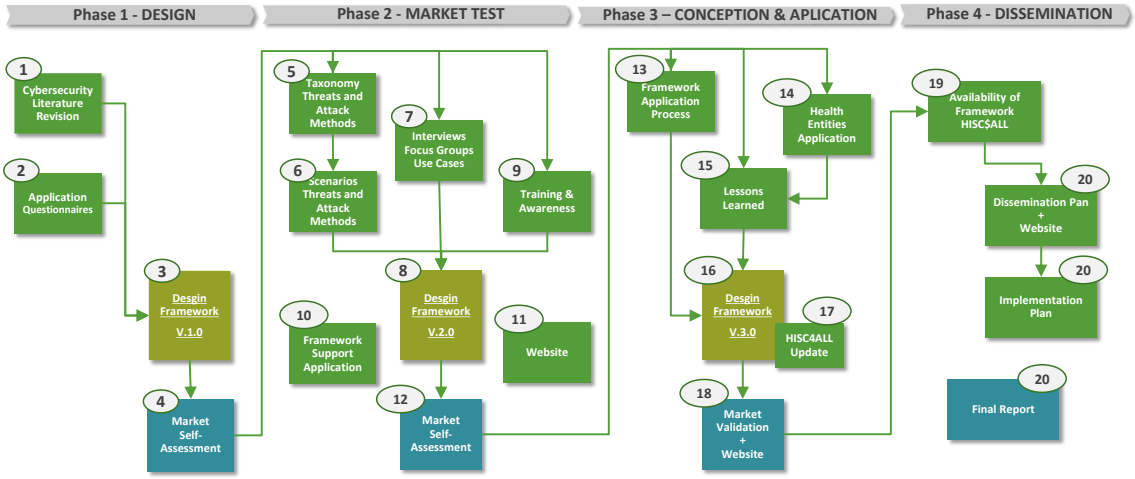
Initial activities by each WORK PACKAGES:

1. DESIGN	2. MARKET TEST	3. CONCEPTION & APPLICATION	4. DISSEMINATION
Activity 1. Literature review and document analysis of the main national and international approaches to Information Security and Cybersecurity **Activity 2**. Application of questionnaires and interviews to the Intervening Entities. **Activity 3**. Security Controls Framework Design (v1.0): Security Dimensions and Dimensional Controls. **Activity 4**. Market Self-Assessment (I)	**Activity 5**. Analyse, obtain or develop a taxonomy of threats/attack methods. **Activity 6**. Build and describe the main attack method scenarios / scenarios **Activity 7**. Perform the Interviews: Focus Group (Uses Cases and requirements specification). **Activity 8**. Design of the Security Controls Framework (v2.0): baselines by security dimension and control maturity levels. **Activity 9**. Training, Awareness and Training Program **Activity 10.** Framework Support Application **Activity 11.** Website **Activity 12**. Market Self Assessment (II)	**Activity 13**. Design of the framework application process. **Activity 14**. Application of the framework to health entities (Action Research – a single cycle) **Activity 15**. Collection of lessons learned. **Activity 16**. Design of the security controls framework (v3.0): security dimensions and controls by dimension. **Activity 17**. HISC4ALL Update **Activity 18**. Market Validation + Website	**Activity 19**. Availability of Framework HISC4ALL **Activity 20**. Final Actions Communication & Dissemination Plan + Website Implementation Plan Final Report

Initial Working Plan & Organization of the Activities

The overall structure of the work plan, with the list of the phases and activities, corresponding to the work packages, and a graphical presentation of the organization of the activities, including the sequence of development of each activity and the connections between them will be developed.

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."



2.5 Initial Activities Description

Project HISC4ALL will be developed in 4 phases, divided into 20 different activities, as presented in the following list and developed through the Work Packages presented in next point.

Phase I (WP1): DESIGN

Activity 1. Literature review and document analysis of the main national and international approaches to Information Security and Cybersecurity relevant to the design of the Health Framework.
It will be delivered considering the premises defined above.

Activity 2. Application of questionnaires and interviews to the Intervening Entities.
Conceiving and applying a set of questions and guided ideas about contend of the framework, to start receiving feedback and information about the needs and expectations.

Activity 3. Security Controls Framework Design (v1.0): Security Dimensions and Dimensional Controls.
Start the conception of the Framework HISC4ALL, considering the knowledge and working methodology described above.

Activity 4. Market Self-Assessment (I)
By inquiring the stakeholders about the first version of the draft framework conceived.
First with INEM, an after in the others beneficiary's stakeholders of the market. Create a database of the tested stakeholders: Hospital and Clinics; Institutions of the Public National Health Service (NHS); SMEs of the healthcare sector (small hospitals, clinics, dentists, pharmacies); Non-profit organizations (Firefighters).

Phase II (WP2): MARKET TEST

Activity 5. Analyse, obtain or develop a taxonomy of threats/attack methods.

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

Define the set of the threats/attacks.

Activity 6. Build and describe the main attack method scenario(s) (use attack method modelling techniques and Use Cases).
Build the scenarios.

Activity 7. Perform the Interviews: Focus Group (Use Cases and requirements specification).
With a guide and oriented results approach, focused in collecting comments and improving suggestions.

Activity 8. Design of the Security Controls Framework (v2.0): baselines by security dimension and control maturity levels.
Continue to develop the HISC4ALL artefacts.

Activity 9. Training, Awareness and Training Program in the implementation and operation of the Framework (v1.0).
Conceiving the capacity & training activities that should be developed to consolidate the implementation of the Framework.

Activity 10. Framework Support Application
Conceive the framework support application.

Activity 11. Website
Develop a first version of the website.

Activity 12. Market Self-Assessment (II)
Apply a market test on the second version of the framework to the selected stakeholders.

Phase III (WP3): CONCEPTION & APPLICATION

Activity 13. Design of the framework application process.
Conceive the framework application process.

Activity 14. Application of the framework to health entities (Action Research – a single cycle)
Presenting the final version to a set of healthcare institutions to validate the outcomes.

Activity 15. Collection of lessons learned.
Register and incorporate the final remarks/suggestions.

Activity 16. Design the security controls framework (v3.0): security dimensions and controls by dimension.

Activity 17. HISC4ALL update
Continuation of the design, start of coding and testing of the Framework Support Application and Implementation Process (HISC4ALL- Website Tool)

Activity 18. Market Validation + Website
Make a final validation and upgrade of the website.

PHASE IV (WP4): DISSEMINATION

Activity 19. Availability of the HISC4ALL Tool

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

Availability of the Framework Support Application and Implementation Process (HISC4ALL Tool - Website v 3.0) Activity 20. Communication & Dissemination Plan + Website

Activity 20. Final actions

Execution of Communication & Dissemination Plan

Develop a plan to communicate and disseminate information to the market about the created Framework, and the conclusion of the HISC4ALL website.

Implementation Plan

Develop a plan for the development of future market and technical applications of the created framework, aiming to improve the process of maturity of the different actors in the health sector involved in sharing data and information, ensuring that these exchanges take place between entities that meet certain minimum-security requirements.

Final Report

Develop the project final report to close the project, including the final versions of:

- Final Framework for Information Security and Cybersecurity;
- Final Training, Awareness and Training program in the implementation and operation of the Framework;
- Final Framework Application Process;
- Framework Operation Process;
- HISC4ALL application (Proof-of-Concept);
- Website.

2.6 Initial Deliverables

Macro deliverables to be presented with the implementation of the global Project.

Deliverables					
Work Package No	**Deliverable Related No**	**Deliverable No**	**Deliverable Name**	**Description**	**Lead Beneficiary**
WP1	D1.1	D1	First Project Report	Document produced in Portuguese and English	PAHLDATA
WP1	D1.2	D2	(Output: Framework v1.0)	Conceptual Document in Portuguese	PAHLDATA
WP2	D2.1	D3	Second Project Report	Document produced in Portuguese and English	PAHLDATA
WP2	D2.2	D4	Information Security and Cybersecurity Framework v2.0	Conceptual Document in Portuguese.	PAHLDATA
WP2	D2.3	D5	Training, Awareness and Training Program in the implementation	Training.	INEM
WP2	D2.4	D6	Framework support application (example: Website (v 1.0))	Application.	PAHLDATA
WP2	D2.5	D7	Website (v1.0)	Application. Site.	INEM
WP3	D3.1	D8	Third Project Split Report	Third Project Split Report.	PAHLDATA
WP3	D3.2	D9	Information Security and Cybersecurity Framework v3.0	Application.	PAHLDATA
WP3	D3.3	D10	Training, Awareness and Training Program in the implementation	Training.	INEM
WP3	D3.4	D11	Framework support application (example: Website (v 2.0))	Framework.	PAHLDATA
WP3	D3.5	D12	Website (v2.0)	Website.	INEM
WP3	D3.6	D13	Workshop	Workshop.	INEM
WP3	D3.7	D14	Scientific Paper	Development of a Scientific Paper.	PAHLDATA
WP4	D4.1	D15	Final Project Report, including: - Final Framework - Final Training	Final Report.	INEM
WP4	D4.2	D16	Framework Operation Process	Operation Process.	PAHLDATA
WP4	D4.3	D17	HISC4ALL application (proof of concept)	Prof of Concept.	PAHLDATA
WP4	D4.4	D18	Implementation Plan +. Dissemination Plan	Implementation and Dissemination Plan.	PAHLDATA
WP4	D4.5	D19	Website 4.0	Website.	INEM
WP4	D4.6	D20	Webinar	Webinar.	INEM

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

3. Introduction

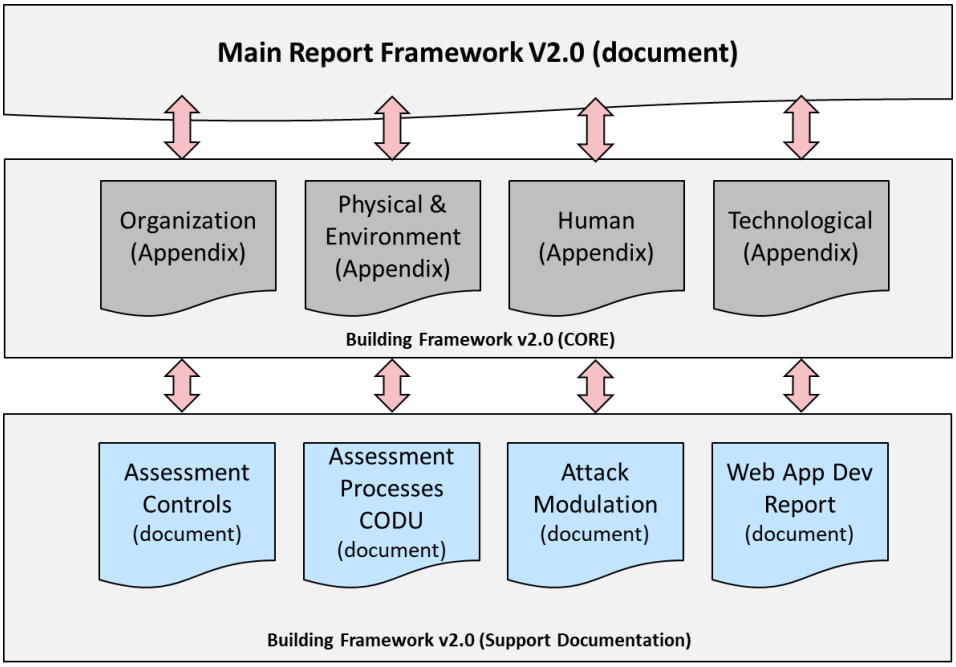
This project report covers the 8-month period relating to Phase II / WP2 of the project. The status of the report will focus on the following points in detail:

- The work that's been completed;
- The plan for what will follow (WP3);
- The summary of the project budget, and schedule;
- A list of action items (milestones and deliveries);
- Issues and risks, and what's being done about them (mitigation).

The main objectives to be achieved in Phase II were:

1. Increase and improve the framework's document base, in terms of its content;
2. To carry out assessments of health institutions and obtain results to incorporate into the framework;
3. Obtain a first version of the web application that will support the framework.

The following diagram outlines the main blocks of work that guided the activities carried out.



Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

4. Project Status Summary

4.1 Key Accomplishments on WP2

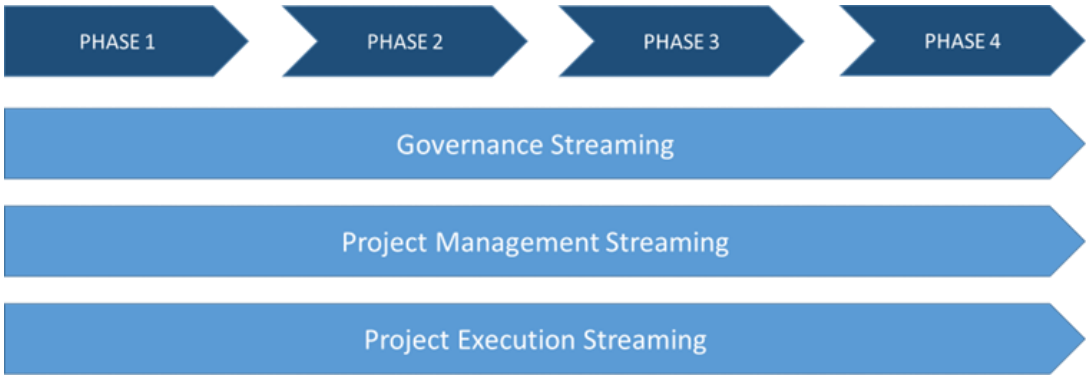
Project Status Summary	
Key Accomplishments	
1	Communication & Dissemination Plan (document)
2	Training, Awareness and Training Program in the implementation and operation of the Framework (v1.0) (document)
3	Framework support application (example: Website (v 1.0)), Software Application (*)
4	Information Security and Cybersecurity Framework v2.0
5	Second Project Report

(*) There is a version (v1.0) of the web application running on Paldata's internal network. A website is also available to communicate and promote the HISC4ALL project (www.hisc4all.com).

4.2 Progress Report

4.2.1 Project Development on Phase II

At the outset of the project, some guiding principles for its governance, management, and execution were established in Project Charter. Accordingly, three operational streams were created:



- STREAM1: Project Governance:
  This stream was created to regulate and control the entire governance of the project. It is used to plan and manage the execution of meetings/steering's at the three levels of governance:

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

Strategic (coordination steering's); Tactical (management steering's); and Operational (execution steering's follow-up).

- STREAM2: Project Management:
  This stream was created to carry out project management according to PMBok (6th edition)/PMI practices, based on the 5 phases and 10 knowledge areas.

- STREAM3: Project Execution:
  This stream materialises the operational activities of the project, in the construction of the framework, the software application that supports it, as well as all the actions necessary for its communication and dissemination inside and outside the project.

These principles currently govern the project, leading to the concretization of the goals and deliverables for Phase I and II.

4.2.2 Completed Work Under WP2

Table of Completed Work (*)			
Action Item	RAG	Owner	Comments
Activities that have been transferred from WP1 to WP2			
1.5 - Planning for Assessment to INEM (WORK FROM WP1)		Paldata	This activity was executed and completed the remaining 80% in WP2
(WITH INEM PARTICIPATION)		INEM	
1.5.1 - Controls (Creation of approaches, methods and plans for assessment) (10 days)		Paldata	
1.5.2 - Use Cases / CODU (Creation of Approaches, Methods and Plans for assessment) (15 days)		Paldata	
1.7 - Perform the INEM Assessment (First Iteration) (WORK FROM WP1)		Paldata	This activity was executed and completed totally in WP2
(WITH INEM PARTICIPATION)		INEM	
1.7.1 - INEM Assessments (Controls + UseCases) (30 days)		Paldata	
1.10 - Integrating the Assessment Outputs into the Framework (4 Dimensions) (WORK FROM WP1) (5 days)		Paldata	This activity was executed and completed totally in WP2
PHASE II – Execution Activities			

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

2.1 - Make available/publish the project's institutional website for consultation		Paldata	
2.2 - Improving the Design of the Framework & Control Model		Paldata	
2.3 - Continue to Literature Review (General Approaches)		Paldata	
2.4 - Continue to Literature Review (Health Approaches)		Paldata	
2.5 - Continue the Academic Literature Review (Health Sector Articles)		Paldata	
2.6 - Planning for Assessment in CHUSJ (WORK NOT DONE)			This activity was not done (**)
2.7 - Finalise the Application Requirements Specification of Web Site Software (v1.0)		Paldata	
2.8 - Execute the Assessment to INEM (Second Iteration)		Paldata	
(WITH INEM PARTICIPATION)		INEM	
2.8.1 - Execute the Assessment		Paldata	
2.9 - Carry out the Assessment in CHUSJ (First Iteration) (WORK NOT DONE)			This activity was not done (**)
2.10 - Continue Defining the Objectives of the Framework Controls		Paldata	
2.11 - Continue Integrating the Assessment Outputs into the Framework (4 Dimensions)		Paldata	
2.12 - Continue Review of Attack Modelling Techniques and Tool Support		Paldata	
2.13 - Continue Literature Review of Framework Utilisation Methods		Paldata	
2.14 - Defining the taxonomy of attack methods and applying them to the reality of healthcare units		Paldata	
2.15 - Drawing up the Framework Awareness and Training Process		Paldata	
2.16 - Analysis, Design and Coding of the Web Site software solution (v1.0)		Paldata	
2.17 - Design of the Information Security and Cybersecurity Baselines, applied to the Framework		Paldata	
2.18 - Apply External activities of Communication and Dissemination Plan		Paldata	
2.19 - Draft the Information Security and Cybersecurity Framework Final Document (v2.0)		Paldata	
2.10 - Create the Second Project Report		Paldata	

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

2.21 - Review of Final Framework Document and Project Report		Paldata	
(WITH INEM PARTICIPATION)		INEM	
(WITH CHUSJ PARTICIPATION)		CHUSJ	
2.21.1 - Review of Final Framework Document and Project Report		Paldata	
PHASE II – Deliverables			
2.22 - Make the Training, Awareness and Coaching model available for FW v1.0		Paldata	
(WITH INEM PARTICIPATION)		INEM	
(WITH CHUSJ PARTICIPATION)		CHUSJ	
2.22.1 - Make the Training, Awareness and Coaching model available		Paldata	
2.23 - Practical application of the Framework to Website v1.0		Paldata	
(WITH INEM PARTICIPATION)		INEM	
(WITH CHUSJ PARTICIPATION)		CHUSJ	
2.23.1 - Practical application of the Framework to Website v1.0 (Show Evidence)		Paldata	
2.24 - Availability of Application Software Web v1.0		Paldata	
2.25 - Prepare for delivery of documentation		Paldata	
(WITH INEM PARTICIPATION)		INEM	
(WITH CHUSJ PARTICIPATION)		CHUSJ	
2.25.1 - Submission of the FRAMEWORK v2.0 document on the EU Portal		Paldata	
2.25.2 - Submission of the Second Project Report on the EU Portal		Paldata	
2.25.3 - Create and upload a HISC4ALL Framework Promotional MEMO in Portal		Paldata	

RAG (Red, Amber, Green)

(*) The activities presented in the table above corresponds to the macro project submitted on initial application, changed to be adapted to the run-away project needs.

(**) With the delay of include CHUSJ in the consortium, this activity was postponed to beginning of 2024

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

4.2.3 Further Work on WP3

Upcaming Work in WP3			
Action Item	RAG	To be done by	Comments
Activities that have been transferred from WP2 to WP3			
2.6 - Planning for Assessment in CHUSJ (WORK NOT DONE)		Paldata and CHUSJ	This activity will be executed and completed in WP3
2.9 - Carry out the Assessment in CHUSJ (First Iteration) (WORK NOT DONE)		Paldata and CHUSJ	This activity will be executed and completed in WP3
PHASE III – Execution Activities			
3.1 - Improving the Design of the Framework & Control Model		Paldata	
3.2 - Continue to Literature Review (General Approaches)		Paldata	
3.3 - Continue to Literature Review (Health Approaches)		Paldata	
3.4 - Continue the Academic Literature Review (Health Sector Articles)		Paldata	
3.5 - Planning the Application of the Framework to Health Units (Action Research)		Paldata	
(WITH INEM PARTICIPATION)		INEM	
(WITH CHUSJ PARTICIPATION)		CHUSJ	
3.5.1 - Planning the Application to Health Units (Action Research)		Paldata	
3.6 - Improving the Application Requirements Specification (Limitations and Future)		Paldata	
3.7 - Execute the CHUSJ Health Unit Assessment (Second Iteration)		Paldata	
(WITH CHUSJ PARTICIPATION)		CHUSJ	
3.7.1 - Execute the CHUSJ Assessment (Second Iteration)		Paldata	
3.8 - Applying the Framework to the Health Unit (Action Research)		Paldata	
(WITH INEM PARTICIPATION)		INEM	
(WITH CHUSJ PARTICIPATION)		CHUSJ	
3.8.1 - Execute on Health Unit (Action Research)		Paldata	
3.9 - Continue Definition and Objectives of Framework Controls		Paldata	
3.10 - Further integration of assessment outputs into the framework		Paldata	
3.11 - Continue Review of Attack Modelling Techniques and Tool Support		Paldata	
(WITH INEM PARTICIPATION)		INEM	

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

(WITH CHUSJ PARTICIPATION)		CHUSJ	
3.11.1 - Review of Attack Modelling Techniques and Tool Support		Paldata	
3.12 - Continue Literature Review of Methods for Using Frameworks		Paldata	
3.13 - Finalise the Taxonomy of Attack Methods and Apply it to the Reality of Healthcare Units		Paldata	
(WITH INEM PARTICIPATION)		INEM	
(WITH CHUSJ PARTICIPATION)		CHUSJ	
3.13.1 - Finalise the Taxonomy of Attack Methods		Paldata	
3.14 - Finalise the Information Security and Cybersecurity Baselines		Paldata	
3.15 - Improving the Awareness and Training Process with the Framework v2.0		Paldata	
(WITH INEM PARTICIPATION)		INEM	
(WITH CHUSJ PARTICIPATION)		CHUSJ	
3.15.1 - Improving the Awareness and Training Process		Paldata	
3.16 - Application Software Analysis, Design and Coding - Web Site (v2.0)		Paldata	
3.17 - Prepare support manuals for administrators and users		Paldata	
(WITH INEM PARTICIPATION)		INEM	
(WITH CHUSJ PARTICIPATION)		CHUSJ	
3.17.1 - Develop support manuals for administrators and users		Paldata	
3.18 - Planning and Designing a Public Workshop		Paldata	
(WITH CHUSJ PARTICIPATION)		CHUSJ	
3.18.1 - Planning the Public Workshop		Paldata	
3.19 - Apply activities of Communication and Dissemination Plan		All	
3.19.1 - Activity 1 (Academic Article / Conference in Finland (27 and 20 June - 2024))		Paldata	
3.19.2 - Activity 2 (BENCHMARK / CODU + URGENCIAS)		Paldata	
3.19.3 - Activity 3 (Workshop - Validation / National)		Paldata	
3.19.4 - Activity 4 (Specialists Panel / National - International)		Paldata	
3.20 - Draft the Information Security and Cybersecurity Framework Final Document (v3.0) , and Project Report		Paldata	
(WITH INEM PARTICIPATION)		INEM	
(WITH CHUSJ PARTICIPATION)		CHUSJ	
3.20.1 - Develop Draft the Information Security and Cybersecurity Framework Final Document (v3.0), and Project Report		Paldata	

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

3.21 - Review of Final Framework Document and Project Report		Paldata	
(WITH INEM PARTICIPATION)		INEM	
(WITH CHUSJ PARTICIPATION)		CHUSJ	
3.21.1 - Review Document of Project Report		Paldata	
PHASE III – Deliverables			
3.22 - Delivery of Training, Awareness Programme (FW v2.0)		Paldata	
3.23 - Framework Support Application (Example: Website Software v2.0)		Paldata	
3.24 - Website Application Software v2.0 made available		Paldata	
3.25 - Delivery of evidence of the workshop		Paldata	
3.26 - Delivery of Scientific Article (Submission evidence)		Paldata	
3.27 - Delivery of FRAMEWORK document (v3.0) on the EU Portal		Paldata	
3.28 - Submission of the Third Project Report on the EU Portal		Paldata	
3.29 - Create and upload a HISC4ALL Framework Promotional MEMO in Portal		Paldata	

RAG (Red, Amber, Green)

4.2.4 Project deliverables of WP2

Project deliverables				
Deliverable Description	Date/Month	RAG	Owner	Comments
Communication & Dissemination Plan	June 2023		INEM	Prepared on June and delivered on July
Training, Awareness and Training Program in the implementation and operation of the Framework (v1.0)	October 2023		INEM	Prepared on October and delivered on November
Framework support application (example: Website (v 1.0))	October 2023		Paldata	Prepared on October and delivered on November
Website (v1.0)	October 2023		INEM	Prepared on October and delivered on November
Information Security and Cybersecurity Framework v2.0	December 2023		Paldata	Prepared on December and delivered on January
Second Project Report	December 2023		Paldata	Prepared on December and delivered on January

RAG (Red, Amber, Green)

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

4.2.5 Project Milestones to WP2

Project Milestones				
Milestone Description of WP's	Date/Month	RAG	Owner	Comments
Theoretic Framework based on Literature review	April 2023		Paldata	Delivered without the INEM initial Assessment
Framework enhanced with defined use cases	December 2023		Paldata	1. INEM Assessment Included and delivered in WP2. 2. CHUSJ Assessment transferred to AP3 (*)

RAG (Red, Amber, Green)

(*) CHUSJ began working on the project in June but was only formally included in the consortium in October 2023.

5. Project Health

5.1 Project Scope Overview

In the context of the research and development project, the scope continues to be that identified in the pre-application/submission phase.

However, some activities have been added and adjusted in the context of the project's Communication and Dissemination, adding events and the publication of documentation that was not identified in the project's preparation.

5.2 Project Schedule Overview

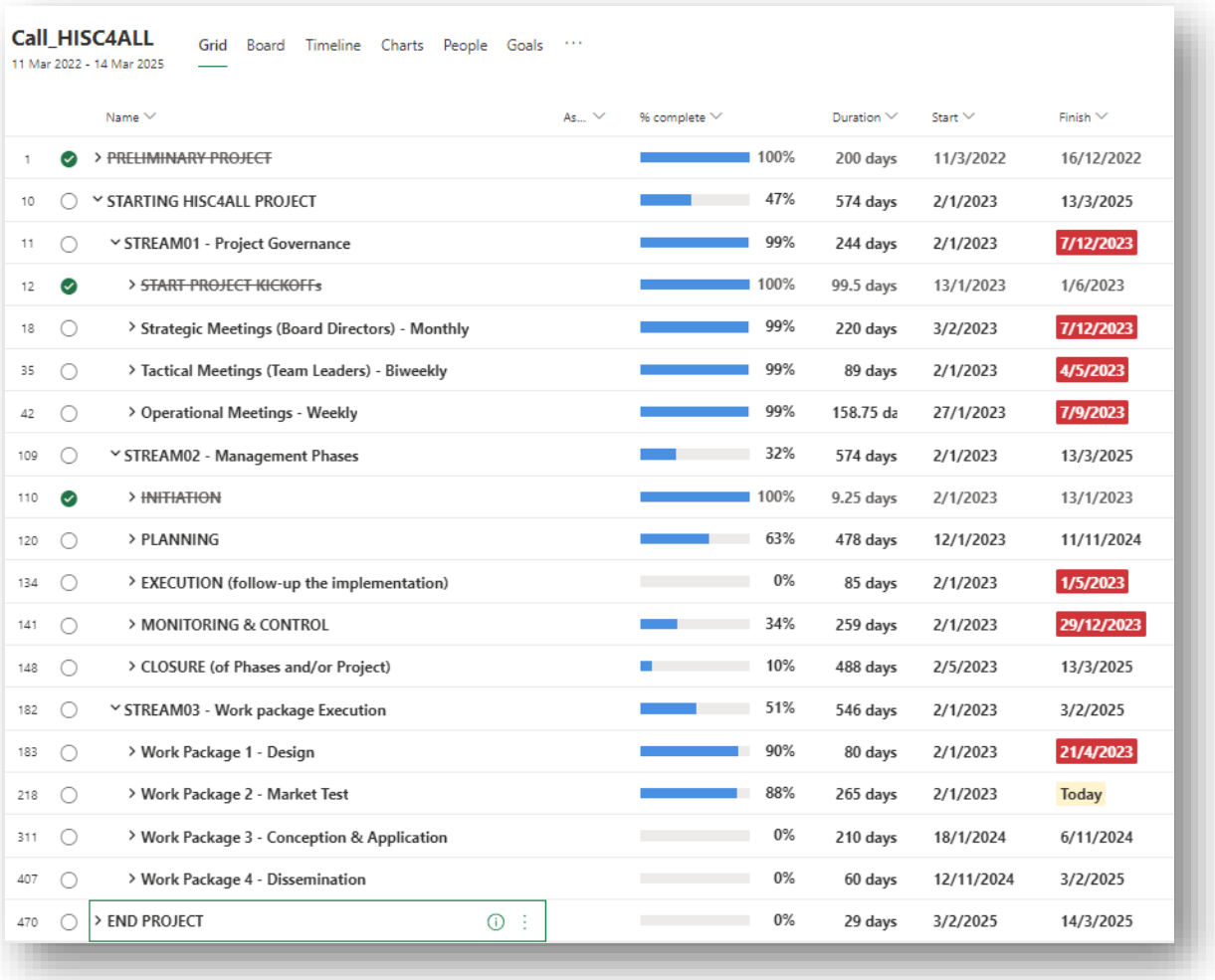
The project timetable to date has undergone minor changes, as shown in the table below:

Changes on Schedule Overview			
Action Item	RAG	Owner	Comments
Activities that have been transferred from WP1 to WP2			
1.5 - Planning for Assessment to INEM (WORK FROM WP1)		Paldata	This activity was started in WP1 20%, and completed the remaining 80% in WP2
(WITH INEM PARTICIPATION)		INEM	
1.5.1 - Controls (Creation of approaches, methods and plans for assessment) (10 days)		Paldata	

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

1.5.2 - Use Cases / CODU (Creation of Approaches, Methods and Plans for assessment) (15 days)		Paldata	
1.7 - Perform the INEM Assessment (First Iteration) (WORK FROM WP1)		Paldata	This activity was started in WP2, and completed in WP2
(WITH INEM PARTICIPATION)		INEM	
1.7.1 - INEM Assessments (Controls + UseCases) (30 days)		Paldata	
1.10 - Integrating the Assessment Outputs into the Framework (4 Dimensions) (WORK FROM WP1) (5 days)		Paldata	This activity was started in WP2, and completed in WP2
Activities that will be transferred from WP2 to WP3			
2.6 - Planning for Assessment in CHUSJ (WORK NOT DONE)			This activity was not done in WP2 was postponed to WP3
2.9 - Carry out the Assessment in CHUSJ (First Iteration) (WORK NOT DONE)			This activity was not done in WP2 was postponed to WP3

The project continues to have the following detailed milestones:



	Name	As...	% complete	Duration	Start	Finish
1	~~PRELIMINARY PROJECT~~		100%	200 days	11/3/2022	16/12/2022
10	STARTING HISC4ALL PROJECT		47%	574 days	2/1/2023	13/3/2025
11	STREAM01 - Project Governance		99%	244 days	2/1/2023	7/12/2023
12	~~START PROJECT KICKOFFs~~		100%	99.5 days	13/1/2023	1/6/2023
18	Strategic Meetings (Board Directors) - Monthly		99%	220 days	3/2/2023	7/12/2023
35	Tactical Meetings (Team Leaders) - Biweekly		99%	89 days	2/1/2023	4/5/2023
42	Operational Meetings - Weekly		99%	158.75 da	27/1/2023	7/9/2023
109	STREAM02 - Management Phases		32%	574 days	2/1/2023	13/3/2025
110	~~INITIATION~~		100%	9.25 days	2/1/2023	13/1/2023
120	PLANNING		63%	478 days	12/1/2023	11/11/2024
134	EXECUTION (follow-up the implementation)		0%	85 days	2/1/2023	1/5/2023
141	MONITORING & CONTROL		34%	259 days	2/1/2023	29/12/2023
148	CLOSURE (of Phases and/or Project)		10%	488 days	2/5/2023	13/3/2025
182	STREAM03 - Work package Execution		51%	546 days	2/1/2023	3/2/2025
183	Work Package 1 - Design		90%	80 days	2/1/2023	21/4/2023
218	Work Package 2 - Market Test		88%	265 days	2/1/2023	Today
311	Work Package 3 - Conception & Application		0%	210 days	18/1/2024	6/11/2024
407	Work Package 4 - Dissemination		0%	60 days	12/11/2024	3/2/2025
470	END PROJECT		0%	29 days	3/2/2025	14/3/2025

Note: The dates in 2025 are used to close the project activities only.

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

5.3 Quality Control & Assurance Overview

Quality control and assurance activities have been carried out within the project management STREAM_2, however it is the intention of the Project Manager and Sponsor to move this area outside of project management and have it taken over by INEM's quality department, in conjunction with project management.

5.4 Risk Management Overview

5.4.1 Initial Risks (submitted application)

Initial risks			
Risk Nr	Description	WP	Proposed Mitigation Measures
1	Unavailability of stakeholders in continuous monitoring of the project	WP1, WP2, WP3, WP4	- Define the work schedule in a timely manner, based on the project planning; - Creation of a steering committee to monitor the project as a whole; - Appointment of a project manager aggregating all entities and definition of a linking element in each participating entity.
2	Delay in the application of questionnaires and conducting interviews	WP1	- Define the work schedule in a timely manner, based on the project planning; - Timely selection of the elements of each participating entity who will be responsible for answering the questionnaires and being subject to interviews.
3	Delay in the execution of the Focus Group	WP2	- Define the work schedule in a timely manner, based on the project planning; - Timely appointment of specialists from each participating entity who will integrate the Focus Group.
4	Delay of the consortium for the application of the Framework, in the defined timeline	WP3	- High-level meetings promoted by the consortium leader to define an integrated strategy that is accepted by all stakeholders; - Timeline redefinition by the consortium leader with the aim of completing the project in the shortest possible time.
5	Delay in delivery of the Application (proof of concept)	WP4	Adjustment of the Application to the functional and non-functional requirements considered a priority within the scope of the consortium and redefining the delivery time line.
6	Not ensuring the Information Security properties (confidentiality, integrity and availability) of the process and outputs resulting from Research and Development (R&D)	WP1, WP2, WP3, WP4	Implement from the beginning, within the scope of project management, a set of security controls that ensure confidentiality, integrity and availability (for example: encrypt all R&D outputs, access to which will be allowed only to certain project profiles).
7	Defining a framework applicable to different countries	WP1, WP2	The literature review will consider current best practices and work developed by distinct entities such as NIS Working Group 12, ENISA and eHealth Network Cybersecurity Guide

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

5.4.2 Actual Risks and Mitigations

Initial risks				
Risk Nr	**Description**	**WP**	**Proposed Mitigation Measures**	**Status/Action**
1	Unavailability of stakeholders in continuous monitoring of the project	WP1, WP2, WP3, WP4	1. Define the work schedule in a timely manner, based on the project planning. 2. Creation of a steering committee to monitor the project as a whole. 3. Appointment of a project manager aggregating all entities and definition of a linking element in each participating entity.	Still having this risk in WP2, the PM is mitigating it with a more rigorous plan control, and governance (*).
2	Delay in the application of questionnaires and conducting interviews	WP1	1. Define the work schedule in a timely manner, based on the project planning. 2. Timely selection of the elements of each participating entity who will be responsible for answering the questionnaires and being subject to interviews.	To plan and execute correctly, the actions on some activities ware transfer to other WP.
3	Delay in the execution of the Focus Group	WP2	1. Define the work schedule in a timely manner, based on the project planning. 2. Timely appointment of specialists from each participating entity who will integrate the Focus Group.	It is controlled and mitigated.
4	Delay of the consortium for the application of the Framework, in the defined timeline	WP3	1. High-level meetings promoted by the consortium leader to define an integrated strategy that is accepted by all stakeholders. 2. Timeline redefinition by the consortium leader with the aim of completing the project in the shortest possible time.	Not yet applied, but controlled.
5	Delay in delivery of the Application (proof of concept)	WP4	Adjustment of the Application to the functional and non-functional requirements considered a priority within the scope of the consortium and redefining the delivery timeline.	Not yet applied, but controlled
6	Not ensuring the Information Security properties (confidentiality, integrity and availability) of the process and outputs resulting from Research and Development (R&D)	WP1, WP2, WP3, WP4	1. Implement from the beginning, within the scope of project management, a set of security controls that ensure confidentiality, integrity and availability (for example: encrypt all R&D outputs, access to which will be allowed only to certain project profiles).	Not yet confirmed, only on WP4
7	Defining a framework applicable to different countries.	WP1, WP2	2. The literature review will consider current best practices and work developed by distinct entities such as NIS Working Group 12, ENISA and eHealth Network Cybersecurity Guide.	Not yet confirmed, only on WP4

(*) As mentioned above, the only real risk was the inclusion of a new element in consortium. That action was done and right now mitigated.

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."

6. Conclusion

It can be concluded that the project as a whole is proceeding according to plan, with the exception of the activities in point "5.2 Project Schedule Overview".

However, the activities relating to WP1 have already been carried out and those relating to WP2 will be carried out at the beginning of 2024.

Funded by the European Union, under grant agreement Nº 101100701
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them."