Digital Europe Programme

(DIGITAL)

Project HISC4ALL

Health Information Safe and Cybersecured for All

First Project Report

Version 1.0

31 May 2023

TABLE OF CONTENTS

1. PROJECT HISC4ALL

1.1. Objectives

Objectives of the Project

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.

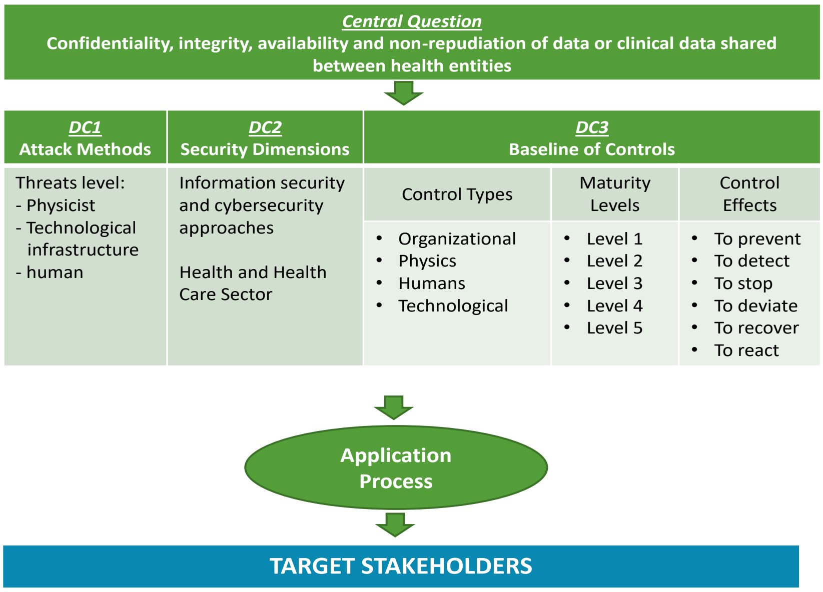
From the central question, **three derived questions** arise that will guide the design of the Framework and later its application process:

(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:



Central Question
Confidentiality, integrity, availability and non-repudiation of data or clinical data shared between health entities

DC1 Attack Methods	*DC2* Security Dimensions	*DC3* Baseline of Controls		
		Control Types	Maturity Levels	Control Effects
Threats level: - Physicist - Technological infrastructure - human	Information security and cybersecurity approaches Health and Health Care Sector	• Organizational • Physics • Humans • Technological	• Level 1 • Level 2 • Level 3 • Level 4 • Level 5	• To prevent • To detect • To stop • To deviate • To recover • To react

Application Process

TARGET STAKEHOLDERS

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.

- *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.*

1.2. Activities

Initial Project Activities

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.

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

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.

1.3. Work Packages

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

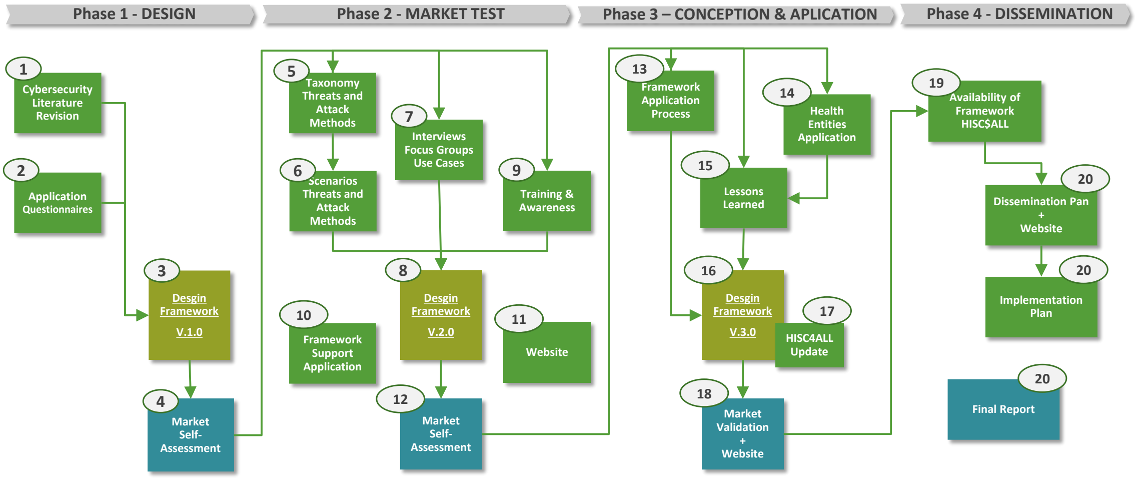
- Work Package 1 – DESIGN
- Work Package 2 – MARKET TEST
- Work Package 3 – CONCEPTION & APLICATION
- Work Package 4 – DISSEMINATION

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

<u>Initial Working Plan & Organization of the Activities</u>

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.


Phase 1 - DESIGN
Phase 2 - MARKET TEST
Phase 3 – CONCEPTION & APLICATION
Phase 4 - DISSEMINATION
1
Cybersecurity Literature Revision
2
Application Questionnaires
3
Desgin Framework V.1.0
4
Market Self-Assessment
5
Taxonomy Threats and Attack Methods
6
Scenarios Threats and Attack Methods
7
Interviews Focus Groups Use Cases
8
Desgin Framework V.2.0
9
Training & Awareness
10
Framework Support Application
11
Website
12
Market Self-Assessment
13
Framework Application Process
14
Health Entities Application
15
Lessons Learned
16
Desgin Framework V.3.0
17
HISC4ALL Update
18
Market Validation + Website
19
Availability of Framework HISC$ALL
20
Dissemination Pan + Website
20
Implementation Plan
20
Final Report

1.4. 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

2. CONSORTIUM

2.1. Consortium in the Application

Consortium Composition in the Agreement date

The Consortium is composed 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. 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;
- 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.

Pahldata – 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. Pahldata 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. Add a New Beneficiary to Consortium

The Consortium created between INEM and Pahldata has as its object the execution of the HISC4All - *Health Information Safe and Cybersecured for All* project.

The Consortium Leader is INEM, and it is responsible for organizing cooperation and technical coordination between the parties in carrying out the Consortium's object, as well as promoting the necessary measures for the execution of the project.

Externally, it is up to the Consortium Leader, through the Project Director, to represent the interests of the Consortium Members within the scope of the project, being granted by the parties the powers to represent the consortium in the award of the contract, in the development and execution of the project.

The Consortium Members will grant the Consortium Leader the powers that, in each case, are necessary for the exercise its functions, by means of an appropriate legal instrument.

Consortium Members undertake to provide the Consortium Leader:

(1) All information necessary to resolve technical or consortium issues;

(2) All elements, documents and actions necessary to fulfil the contract;

(3) All information necessary to monitor and control the project;

(4) Information about the progress of the works;

(5) Information about any change or occurrence that jeopardizes the assumptions on which the project was approved, as well as its punctual implementation.

Consortium Members are jointly responsible for the execution of the project, as well as for delays or imperfections of the project as a whole, being obliged to take appropriate measures to fill the gaps and mitigate the effects of those shortcomings.

However, each Consortium Member is only liable for the service it is responsible for, under the terms of the approved or subsequently amended project.

Thus, in internal relations, each Consortium Member is responsible for any delays or imperfections that are occurring during the execution of the work and undertakes to recover them by itself or at its own expense.

Comment

The initial consortium had three members at the time of the first application's submission; however, the contract was reduced to two members in December 2022, by administrative reasons.

To fulfil the scope of the initial application, the consortium suggests adding a third beneficiary member—a public sector hospital. In order to achieve this goal, the consortium opened in the EU portal an amendment, kicking off the inclusion procedure.

2.3. 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;
- ✓ 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.

3. PROJECT EXECUTION

At the outset of the project, some guiding principles for its governance, management, and execution were established. Accordingly, three operational streams were created: STREAM1: Project Governance; STREAM2: Project Management; STREAM3: Project Execution.

These principles currently govern the project, leading to the concretization of the goals and deliverables for Phase 1.

3.1. WORK DEVELOPED (STREAM3) IN WP1

3.1.1. Planned Execution Activities

Although the project's phases remain in the time frames initially identified in the application, the activities associated with those phases have undergone adjustments to better fit the completion of phase 1.

The actual activities that were carried out as planned are listed below.

Work Package 1 – Framework Design

EXECUTION ACTIVITIES

WP1.1 - Conception of the Framework structure and Control Model

WP1.2 - Literature Review (General approaches / Frameworks, etc.)

WP1.3 - Literature Review (Health Approaches / Frameworks, etc.)

WP1.4 - Review of Academic Literature (Health Sector Articles)

WP1.5 – General Plan for INEM Assessment

WP1.6 – Software Application Requirements Specification

WP1.7 - Execution of the INEM Assessment (First Iteration)

WP1.8 - Definition and Objectives of the Framework's Categories and Controls (4 Dimensions)

WP1.9 - Integration of Categories/Controls in a Four-Dimensional Framework scope

WP1.10 - Integration of Assessment Outputs into Framework (4 Dimensions)

WP1.11 - Review of Attack Modelling Techniques and Tool Support

WP1.12 - Review of Framework Utilization Methodology Literature

WP1.13 - Analyse and Choose Supportive Software (UML, Attack Modelling, and Vulnerability Assessment)

WP1.14 - Create the Framework for Information Security and Cybersecurity's Final Document (v1.0)

WP1.15 - Final Framework Document Revision

DELIVERABLES

WP1.16 - Prepare the documentation to be delivered

WP1.17 - Delivery of the FRAMEWORK v1.0 - EU document

WP1.18 - Delivery of the project's initial report to the EU

3.1.2. Work Performed and Developed Activities

The completed work corresponded to most of the activities. Only the previously underlined activities were not completed in full or in partial. The proportion of completion of these activities is described below.

Activities that were only partially or not completely completed will be moved to the second phase (WP2).

WP1.5 –	General Plan for INEM Assessment

Completion: 20%

WP1.7 -	Execution of the INEM Assessment (First Iteration)

Completion: 0%

WP1.10 -	Integration of Assessment Outputs into Framework (4 Dimensions)

Completion: 0%

Reasons for non-conclusion of the activities:

The real involvement of the INEM's project and operational/business teams took longer than expected, causing a delay in these activities.

However, the teams are operational and fully engaged in project activities to finish the WP1 delayed activities and perform the WP2 activities.

3.1.3. Main Achievements

1. Engage the identified stakeholders;
2. Execution of the generality of the planned activities;
3. Full delivery of Version 1 of the Framework on the specified date, as defined in the agreement.

3.1.4. Results and Impacts

The outcomes obtained in Phase 1 were as expected, resulting in a positive impact on Phase 2, since it provides the conditions for carrying out the activities planned for Phase 2 without critical dependencies.

3.1.5. Improvements and Adjustments

Improve the management of the three Streams (Governance, Management and Execution), as well as a better allocation of activities and resources for all teams.

3.2. PLANNING THE DEVELOPMENT OF WP2

3.2.1. Execution activities to be developed

Work Package 2 – Market Test

EXECUTION ACTIVITIES

WP2.1 - Improving Framework Model Conception and Control

WP2.2 - Continue with Literature Review (General Approaches)

WP2.3 - Continue with Literature Review (Health Approaches)

WP2.4 - Continue the Review of Academic Literature (Health Sector Articles)

WP2.5 - Plan the Assessment of the other Health Service Units (US) X and Y

WP2.6 - Complete the Application Requirements Specification

WP2.7 - Carry out the INEM assessment (first and second iteration)

WP2.8 - Conduct Assessments at Units X and Y (first Iteration)

WP2.9 - Continue with the Definition and Objectives of the Framework Controls

WP2.10 - Continue integrating assessment outputs into the Framework

WP2.11 - Continue the Review of Attack Modelling Techniques and Tool Support

WP2.12 - Continue the review of literature on Framework Use Methods

WP2.13 - Create the Framework's Final Document on Information Security and Cybersecurity (v2.0)

WP2.14 - Framework Final Document Review (v2.0)

WP2.15 - Define the taxonomy of attack methods and apply them to the reality of the Health Units

WP2.16 - Create a Sensibilization and Training Process Using the Framework

WP2.17 - Application Analysis, Design, and Codification - Web Site (v1.0)

WP2.18 - Recognition of Information Security and Cybersecurity Baselines

DELIVERABLES

WP2.19 - Delivery of the FRAMEWORK v2.0 document to the EU

WP2.20 - Delivery of the Training Program, Sensibilization FW v1.0

WP2.21 - Application of the Framework to the Website v1.0

WP2.22 - Availability of the Web Application v1.0

WP2.23 - Delivery of the Second Project Report to the EU

Lisbon, May 31, 2023

Coordination of HISC4ALL