EUROPEAN COMMISSION
Directorate-General for Communications Networks, Content and Technology

CNECT.H – Digital Society, Trust and Cybersecurity
H.1 – Cybersecurity Technology and Capacity Building

AMENDMENT No AMD-101100701-1

Project: 101100701 — HISC4ALL

The parties agree to amend the Agreement as follows ('**Amendment**'):

1 . Addition of a new beneficiary

The following new beneficiary is added as from:

- CENTRO HOSPITALAR DE SAO JOAO EPE (CHSJP): 1 June 2023

This implies the **following changes** to the Agreement:

- The new beneficiary and the entry date are added to the list of participants in the **Data Sheet**.
- The new beneficiary is added to the **Preamble**:
  - 3. **CENTRO HOSPITALAR DE SAO JOAO EPE (CHSJP),** PIC 969128456, established in ALAMEDA DO PROFESSOR HERNANI MONTEIRO, PORTO 4200 319, Portugal

2 . Change of Annex 1

Annex 1 is changed and replaced by the Annex 1 attached to this Amendment.

3. Change of Annex 2

The estimated budget in **Annex 2** is changed.

This implies the **following changes** to the Agreement:

- **Annex 2** is changed and replaced by the Annex 2 attached to this Amendment.
- The table on maximum grant amount and total estimated eligible costs and contributions in the **Data Sheet** is updated.

All other provisions of the Agreement and its Annexes remain unchanged.

This Amendment **enters into force** on the day of the last signature.

This Amendment **takes effect** on the date(s) mentioned in the amendment clause(s) (or — if no date was chosen — on the same date the Amendment enters into force).

Please inform the other members of your consortium (if any) of this Amendment.

SIGNATURES

For the coordinator

Assinado por: **LUÍS ALBERTO RODRIGUES ALVES MEIRA**
Num. de Identificação: 07715656
Data: 2024.03.15 14:36:44+00'00'
Certificado por: **Diário da República**
Atributos certificados: **Presidente do Conselho Diretivo - Instituto Nacional de Emergência Médica, I. P.**

Luís Meira

For the granting authority

Done in English

Enclosures: Grant Agreement Data Sheet
Grant Agreement Annex 1
Grant Agreement Annex 2

European Commission

ANNEX 1

Digital Europe Programme (DIGITAL)

Description of the action (DoA)

Part A

Part B

DESCRIPTION OF THE ACTION (PART A)

COVER PAGE

Part A of the Description of the Action (DoA) must be completed directly on the Portal Grant Preparation screens.

PROJECT *Grant Preparation (General Information screen) — Enter the info.*	
Project number:	101100701
Project name:	Health Information Safe and Cybersecured for All
Project acronym:	HISC4ALL
Call:	DIGITAL-2022-CYBER-02
Topic:	DIGITAL-2022-CYBER-02-SUPPORTHEALTH
Type of action:	DIGITAL-SME
Service:	CNECT/H/01
Project starting date:	fixed date: 1 January 2023
Project duration:	24 months

TABLE OF CONTENTS

PROJECT SUMMARY

Project summary *Grant Preparation (General Information screen) — Provide an overall description of your project (including context and overall objectives, planned activities and main achievements, and expected results and impacts (on target groups, change procedures, capacities, innovation etc)). This summary should give readers a clear idea of what your project is about.* *Use the project summary from your proposal.*
The Project HISC4ALL – Health Information Safe and Secured for All, consist of creating a FRAMEWORK involving the SME in Design a common and shared Information Security and Cybersecurity Framework for the healthcare sector, and its application process. The promoters are Instituto Nacional de Emergência Médica (INEM)–Public Institution from the Ministry of Health, responsible for the Integrated Medical Emergency System; Hospital Lusíadas, Private Hospital; and QUATTRO–Private SME, Health Sector Information Solutions Provider. Covid-19 pandemic made a sudden and urgent shifted of the patient care to citizens' homes, making the Healthcare entities more exposed to cyber-attacks. The Consortium saw the need in the market to incorporate a Information Security and Cybersecurity tool. It gives to the market a personalized service of monitoring, detection, and response to security incidents, operated by a team of specialists, based on a set of technological solutions, and supported by standards and frameworks to ensure the compliance of the service. The Consortium propose to create a new framework to assess the level of maturity of the different actors in the health sector involved in sharing data and information with and within each other. The purpose is to ensure that these exchanges take place between entities that meet certain minimum-security requirements and, to this end, comply with the highest levels of the maturity model to be developed. Outcomes will be: 1)Final Framework for Information Security and Cybersecurity; 2)Final Training, Awareness and Training program in the implementation and operation of the Framework; 3)Final Framework Application Process; 4)Framework Operation Process; 5)HISC4ALL application (proof of concept); 6)Website. The target Stakeholders are 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).

LIST OF PARTICIPANTS

PARTICIPANTS

Grant Preparation (Beneficiaries screen) — Enter the info.

Number	Role	Short name	Legal name	Country	PIC
1	COO	INEM	INEM	PT	940442840
2	BEN	PAHLDATA	PAHLDATA (PORTUGAL) - COMERCIO DE EQUIPAMENTO DE INFORMATICA S.A.	PT	893426940
3	BEN	CHSJP	CENTRO HOSPITALAR DE SAO JOAO EPE	PT	969128456

LIST OF WORK PACKAGES

Work packages

Grant Preparation (Work Packages screen) — Enter the info.

Work Package No	Work Package name	Lead Beneficiary	Effort (Person-Months)	Start Month	End Month	Deliverables
WP1	Design	2 - PAHLDATA	16.80	1	4	D1.1 – First Project Report D1.2 – (Output: Framework v1.0)
WP2	Market Test	1 - INEM	42.30	5	12	D2.1 – Second Project Report D2.2 – Information Security and Cybersecurity Framework v2.0 D2.3 – Training, Awareness and Training Program in the implementation and operation of the Framework (v1.0) D2.4 – Framework support application (example: Website (v 1.0)) D2.5 – Website (v1.0) D2.6 – Communication & Dissemination Plan
WP3	Conception & Application	2 - PAHLDATA	44.70	13	22	D3.1 – Third Project Split Report D3.2 – Information Security and Cybersecurity Framework v3.0 D3.3 – Training, Awareness and Training Program in the implementation and operation of the Framework (v2.0) D3.4 – Framework support application (example: Website (v 2.0)) D3.5 – Website (v2.0) D3.6 – Workshop D3.7 – Scientific Paper
WP4	Dissemination	1 - INEM	11.40	23	24	D4.1 – Final Project Report, including: -

Work packages *Grant Preparation (Work Packages screen) — Enter the info.*						
Work Package No	**Work Package name**	**Lead Beneficiary**	**Effort (Person-Months)**	**Start Month**	**End Month**	**Deliverables**
						Final Framework - Final Training - Final Process D4.2 – Framework Operation Process D4.3 – HISC4ALL application (proof of concept) D4.4 – Implementation Plan +. Dissemination Plan D4.5 – Website 4.0 D4.6 – Webinar

Work package WP1 – Design

Work Package Number	WP1	**Lead Beneficiary**	2 - PAHLDATA
Work Package Name	Design		
Start Month	1	**End Month**	4

Objectives
Design of the Information Security and Cybersecurity Framework (dimensions, baselines and security controls) based on the literature review, the professional experience of the team and the questionnaires and interviews developed. Conducting a first market test.

Description
1- State of the Art (Cybersecurity Literature Revision): Literature review and document analysis of the main national and international approaches to Information Security and Cybersecurity relevant to the design of the Framework. 2 - Market Research (Application Questionnaires: Application of questionnaires and interviews to the Intervening Entities. 3 - Framework Design V1.0: Security Controls Framework Design (v1.0): Security Dimensions and Dimensional Controls. 4 - Market Self-Assessment: Market Self-Assessment (I)

Work package WP2 – Market Test

Work Package Number	WP2	**Lead Beneficiary**	1 - INEM
Work Package Name	Market Test		
Start Month	5	**End Month**	12

Objectives
- Build and describe the main attack method scenarios for the Use Cases defined for the healthcare area. - Improved the design of the Information Security and Cybersecurity Framework (v2.0) - Develop the awareness and training program for the implementation and use of the Framework (v1.0). - Analysis and Design of the Framework Support Application

Description
5. Analyse, obtain or develop a taxonomy of threats/attack methods. 6. Build and describe the main attack method scenarios / scenarios (use attack method modelling techniques and Use Cases). 7. Perform the Interviews: Focus Group (Uses Cases and requirements specification). 8. Communication & Dissemination Plan 9. Design of the Security Controls Framework (v2.0): baselines by security dimension and control maturity levels. 10. Training, Awareness and Training Program in the implementation and operation of the Framework (v1.0). 11. Framework Support Application 12. Website 13. Market Self-Assessment (II)

Work package WP3 – Conception & Application

Work Package Number	WP3	**Lead Beneficiary**	2 - PAHLDATA
Work Package Name	Conception & Application		

Start Month	13	**End Month**	22

Objectives
- Design of the framework application process. - Implement the application of the Framework in health entities and collect lessons learned. - Improved the preparation of the Training, Awareness and Training program in the implementation and operation of the Framework (v2.0). - Design, Coding, testing of the Framework Support Application (v2.0).

Description
14 - Framework Application Process: Design of the framework application process. 15 - Action Research - Health Entities Application: Application of the framework to health entities 16 - Lessons Learned: Collection of lessons learned 17 - Desgin Framework V.3.0: Design of framework (v3.0) 18 - HISC4ALL update: Continuation of the design, start of coding and testing of the Framework Support Application and Implementation Process (HISC4ALL- Website Tool) 19 - Website update + Market Validation: Website Update + Market Validation

Work package WP4 – Dissemination

Work Package Number	WP4	**Lead Beneficiary**	1 - INEM
Work Package Name	Dissemination		
Start Month	23	**End Month**	24

Objectives
- Review and Validation of the final Information Security and Cybersecurity Framework. - Review and Validation of the final Training, Awareness and Training Program in the implementation and operation of the Framework. - Review and Validation of the Final Framework Application Process - Review and Validation of the Final Framework Application Process - Review and Validation of the HISC4ALL Application (proof of concept).

Description
20 - Delivering and make availability of the HISC4All Tool: Availability of the Framework Support Application and Implementation Process (HISC4ALL Tool - Website v 3.0) 21 - Communication Plan + Website Update v3.0: Update of the Pojeto website and elaboration of the communication and dissemination plan of the Framework in the post-project 22 -Implementation Plan: Preparation of the plan to follow up on the Framework design project carried out 23 - Final Report + Translations: Final report

STAFF EFFORT

Staff effort per participant

Grant Preparation (Work packages - Effort screen) — Enter the info.

Participant	WP1	WP2	WP3	WP4	Total Person-Months
1 - INEM	4.80	7.90	6.60	3.30	22.60
2 - PAHLDATA	12.00	24.50	23.90	7.20	67.60
3 - CHSJP		9.90	14.20	0.90	25.00
Total Person-Months	16.80	42.30	44.70	11.40	115.20

LIST OF DELIVERABLES

Deliverables

Grant Preparation (Deliverables screen) — Enter the info.

The labels used mean:

Public — fully open (⚠ automatically posted online)
Sensitive — limited under the conditions of the Grant Agreement
EU classified —RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision [2015/444](2015/444)

Deliverable No	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month)
D1.1	First Project Report	WP1	2 - PAHLDATA	R — Document, report	SEN - Sensitive	4
D1.2	(Output: Framework v1.0)	WP1	2 - PAHLDATA	R — Document, report	SEN - Sensitive	4
D2.1	Second Project Report	WP2	2 - PAHLDATA	R — Document, report	SEN - Sensitive	12
D2.2	Information Security and Cybersecurity Framework v2.0	WP2	2 - PAHLDATA	R — Document, report	SEN - Sensitive	12
D2.3	Training, Awareness and Training Program in the implementation and operation of the Framework (v1.0)	WP2	1 - INEM	R — Document, report	SEN - Sensitive	9
D2.4	Framework support application (example: Website (v 1.0))	WP2	2 - PAHLDATA	DEM — Demonstrator, pilot, prototype	SEN - Sensitive	10
D2.5	Website (v1.0)	WP2	1 - INEM	DEC —Websites, patent filings, videos, etc	PU - Public	10
D2.6	Communication & Dissemination Plan	WP2	1 - INEM	R — Document, report	PU - Public	6
D3.1	Third Project Split Report	WP3	2 - PAHLDATA	R — Document, report	SEN - Sensitive	22
D3.2	Information Security and Cybersecurity Framework v3.0	WP3	2 - PAHLDATA	R — Document, report	SEN - Sensitive	22
D3.3	Training, Awareness and Training Program	WP3	1 - INEM	R — Document, report	SEN - Sensitive	16

Deliverables

Grant Preparation (Deliverables screen) — Enter the info.

The labels used mean:

Public — fully open (⚠ automatically posted online)
Sensitive — limited under the conditions of the Grant Agreement
EU classified —RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision 2015/444

Deliverable No	**Deliverable Name**	**Work Package No**	**Lead Beneficiary**	**Type**	**Dissemination Level**	**Due Date (month)**
	in the implementation and operation of the Framework (v2.0)					
D3.4	Framework support application (example: Website (v 2.0))	WP3	2 - PAHLDATA	DEM — Demonstrator, pilot, prototype	PU - Public	20
D3.5	Website (v2.0)	WP3	1 - INEM	DEC —Websites, patent filings, videos, etc	PU - Public	22
D3.6	Workshop	WP3	3 - CHSJP	OTHER	PU - Public	20
D3.7	Scientific Paper	WP3	2 - PAHLDATA	OTHER	SEN - Sensitive	20
D4.1	Final Project Report, including: - Final Framework - Final Training - Final Process	WP4	1 - INEM	R — Document, report	PU - Public	24
D4.2	Framework Operation Process	WP4	2 - PAHLDATA	R — Document, report	SEN - Sensitive	24
D4.3	HISC4ALL application (proof of concept)	WP4	2 - PAHLDATA	R — Document, report	SEN - Sensitive	24
D4.4	Implementation Plan +. Dissemination Plan	WP4	3 - CHSJP	R — Document, report	SEN - Sensitive	24
D4.5	Website 4.0	WP4	1 - INEM	DEC —Websites, patent filings, videos, etc	PU - Public	24
D4.6	Webinar	WP4	3 - CHSJP	OTHER	PU - Public	24

Deliverable D1.1 – First Project Report

Deliverable Number	D1.1	**Lead Beneficiary**	2 - PAHLDATA
Deliverable Name	First Project Report		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	4	**Work Package No**	WP1

Description
Document produced in Portuguese and English with an update of the project and project management.

Deliverable D1.2 – (Output: Framework v1.0)

Deliverable Number	D1.2	**Lead Beneficiary**	2 - PAHLDATA
Deliverable Name	(Output: Framework v1.0)		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	4	**Work Package No**	WP1

Description
Conceptual Document in Portuguese

Deliverable D2.1 – Second Project Report

Deliverable Number	D2.1	**Lead Beneficiary**	2 - PAHLDATA
Deliverable Name	Second Project Report		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	12	**Work Package No**	WP2

Description
Document produced in Portuguese and English with an update of the project and project management.

Deliverable D2.2 – Information Security and Cybersecurity Framework v2.0

Deliverable Number	D2.2	**Lead Beneficiary**	2 - PAHLDATA
Deliverable Name	Information Security and Cybersecurity Framework v2.0		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	12	**Work Package No**	WP2

Description
Conceptual Document in Portuguese.

Deliverable D2.3 – Training, Awareness and Training Program in the implementation and operation of the Framework (v1.0)

Deliverable Number	D2.3	**Lead Beneficiary**	1 - INEM
Deliverable Name	Training, Awareness and Training Program in the implementation and operation of the Framework (v1.0)		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	9	**Work Package No**	WP2

Description
Training.

Deliverable D2.4 – Framework support application (example: Website (v 1.0))

Deliverable Number	D2.4	**Lead Beneficiary**	2 - PAHLDATA
Deliverable Name	Framework support application (example: Website (v 1.0))		
Type	DEM — Demonstrator, pilot, prototype	**Dissemination Level**	SEN - Sensitive
Due Date (month)	10	**Work Package No**	WP2

Description
Application.

Deliverable D2.5 – Website (v1.0)

Deliverable Number	D2.5	**Lead Beneficiary**	1 - INEM
Deliverable Name	Website (v1.0)		
Type	DEC —Websites, patent filings, videos, etc	**Dissemination Level**	PU - Public
Due Date (month)	10	**Work Package No**	WP2

Description
Application. Site.

Deliverable D2.6 – Communication & Dissemination Plan

Deliverable Number	D2.6	**Lead Beneficiary**	1 - INEM
Deliverable Name	Communication & Dissemination Plan		
Type	R — Document, report	**Dissemination Level**	PU - Public
Due Date (month)	6	**Work Package No**	WP2

Description
Communication & Dissemination Plan

Deliverable D3.1 – Third Project Split Report

Deliverable Number	D3.1	**Lead Beneficiary**	2 - PAHLDATA
Deliverable Name	Third Project Split Report		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	22	**Work Package No**	WP3

Description
Third Project Split Report.

Deliverable D3.2 – Information Security and Cybersecurity Framework v3.0

Deliverable Number	D3.2	**Lead Beneficiary**	2 - PAHLDATA
Deliverable Name	Information Security and Cybersecurity Framework v3.0		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	22	**Work Package No**	WP3

Description
Application.

Deliverable D3.3 – Training, Awareness and Training Program in the implementation and operation of the Framework (v2.0)

Deliverable Number	D3.3	**Lead Beneficiary**	1 - INEM
Deliverable Name	Training, Awareness and Training Program in the implementation and operation of the Framework (v2.0)		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	16	**Work Package No**	WP3

Description
Training.

Deliverable D3.4 – Framework support application (example: Website (v 2.0))

Deliverable Number	D3.4	**Lead Beneficiary**	2 - PAHLDATA
Deliverable Name	Framework support application (example: Website (v 2.0))		
Type	DEM — Demonstrator, pilot, prototype	**Dissemination Level**	PU - Public
Due Date (month)	20	**Work Package No**	WP3

Description
Framework.

Deliverable D3.5 – Website (v2.0)

Deliverable Number	D3.5	**Lead Beneficiary**	1 - INEM
Deliverable Name	Website (v2.0)		
Type	DEC —Websites, patent filings, videos, etc	**Dissemination Level**	PU - Public
Due Date (month)	22	**Work Package No**	WP3

Description
Website.

Deliverable D3.6 – Workshop

Deliverable Number	D3.6	**Lead Beneficiary**	3 - CHSJP
Deliverable Name	Workshop		
Type	OTHER	**Dissemination Level**	PU - Public
Due Date (month)	20	**Work Package No**	WP3

Description
Workshop.

Deliverable D3.7 – Scientific Paper

Deliverable Number	D3.7	**Lead Beneficiary**	2 - PAHLDATA
Deliverable Name	Scientific Paper		
Type	OTHER	**Dissemination Level**	SEN - Sensitive
Due Date (month)	20	**Work Package No**	WP3

Description
Development of a Scientific Paper.

Deliverable D4.1 – Final Project Report, including: - Final Framework - Final Training - Final Process

Deliverable Number	D4.1	**Lead Beneficiary**	1 - INEM
Deliverable Name	Final Project Report, including: - Final Framework - Final Training - Final Process		
Type	R — Document, report	**Dissemination Level**	PU - Public
Due Date (month)	24	**Work Package No**	WP4

Description
Final Report.

Deliverable D4.2 – Framework Operation Process

Deliverable Number	D4.2	**Lead Beneficiary**	2 - PAHLDATA
Deliverable Name	Framework Operation Process		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	24	**Work Package No**	WP4

Description
Operation Process.

Deliverable D4.3 – HISC4ALL application (proof of concept)

Deliverable Number	D4.3	**Lead Beneficiary**	2 - PAHLDATA
Deliverable Name	HISC4ALL application (proof of concept)		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	24	**Work Package No**	WP4

Description
Prof of Concept.

Deliverable D4.4 – Implementation Plan +. Dissemination Plan

Deliverable Number	D4.4	**Lead Beneficiary**	3 - CHSJP
Deliverable Name	Implementation Plan +. Dissemination Plan		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	24	**Work Package No**	WP4

Description
Implementation and Dissemination Plan.

Deliverable D4.5 – Website 4.0

Deliverable Number	D4.5	**Lead Beneficiary**	1 - INEM
Deliverable Name	Website 4.0		
Type	DEC —Websites, patent filings, videos, etc	**Dissemination Level**	PU - Public
Due Date (month)	24	**Work Package No**	WP4

Description
Website.

Deliverable D4.6 – Webinar

Deliverable Number	D4.6	**Lead Beneficiary**	3 - CHSJP
Deliverable Name	Webinar		
Type	OTHER	**Dissemination Level**	PU - Public
Due Date (month)	24	**Work Package No**	WP4

Description
Webinar.

LIST OF MILESTONES

Milestones

Grant Preparation (Milestones screen) — Enter the info.

Milestone No	Milestone Name	Work Package No	Lead Beneficiary	Means of Verification	Due Date (month)
1	Theoretic Framework based on Literature review	WP1	2 - PAHLDATA	Document with framework description	4
2	Framework enhanced with defined use cases	WP2	1 - INEM	Document with framework description updated	12
3	Framework Implementation Process	WP3	2 - PAHLDATA	Document	22
4	HISC4ALL application	WP4	1 - INEM	Online tool	24

LIST OF CRITICAL RISKS

Critical risks & risk management strategy

Grant Preparation (Critical Risks screen) — Enter the info.

Risk number	Description	Work Package No(s)	Proposed Mitigation Measures
1	Unavailability of stakeholders in continuous monitoring of the project	WP4, WP2, WP1, WP3	- 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;

Critical risks & risk management strategy

Grant Preparation (Critical Risks screen) — Enter the info.

Risk number	**Description**	**Work Package No(s)**	**Proposed Mitigation Measures**
			- 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 time line	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)	WP4, WP2, WP1, WP3	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	WP2, WP1	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

ANNEX 1

Digital Europe Programme (DIGITAL)

Description of the action (DoA)

Part B

Version 3.0
31 October 2023

TABLE OF CONTENTS

1. RELEVANCE

1.1 Objectives and activities

Objectives and activities

Describe how the project is aligned with the objectives and activities as described in the Call document.

How does the project address the general objectives and themes and priorities of the call? What is the project's contribution to the overall Digital Europe Programme objectives?

Market Concerns

Today, there is great public concern about the **Cybersecurity in Health Sector**, around the following two topics:

– There is a market concern to develop aspects of **Information Security and Cybersecurity** related to the health sector, both in Portugal and in Europe.
– There is a market concern to guarantee the fundamental security properties – **confidentiality, integrity** and **availability**, and, in the case of health, **non-repudiation.**

In organizations in general, and in healthcare organizations in particular, information (e.g. data/clinical information) is one of the most important assets. Its storage, processing and transmission depend on three main elements: (i) technology, which allows it to be stored, processed and transmitted; (ii) the stakeholders, who can access it through private networks or the Internet; and (iii) the business processes that use it. Thus, one must seek to permanently guarantee the fundamental properties of its security, as identified above: confidentiality, integrity, availability and non-repudiation.

It is noted that **attack methods or malicious actions** consist of the execution of an action or set of actions, by an attacker, to exploit one or more vulnerabilities of a particular asset in an Organization. Vulnerabilities being understood as the weakness of an asset or set of organizational assets. These actions can be carried out and have effects at three levels or dimensions of action (designated in the project as attack vectors), which are the physical, technological infrastructure and human (cognitive) levels.

At the **physical level**, actions on physical facilities, equipment, hardware, critical infrastructure, paper documents, images, videos in analogue format and the organization's employees can be considered as an example.

At the **level of technological infrastructure**, actions can be performed on applications (e.g., operating system, databases) that allow users to manipulate data and produce information. These actions also make it possible to change the operation of the organization's computer network, through internal access or via the Internet, exploiting the vulnerabilities of the implemented services or the communication protocols used. Consequently, the monitoring of actions taken on digital data stored, transmitted or processed in the organization should be a permanent concern of decision-makers.

Finally, the **human level** focuses on the employees who participate in the different activities and tasks of the healthcare organization's value chain support processes. In this way, special attention should be given to actions that make it possible to change decision-making processes, the decision-makers' perception of a given problem or the manipulation of users who interact with the information.

This main market concerns justify the design of a Framework and the respective application process, which it's the base of the project HISC4ALL.

Objectives of the Project

Project HISC4ALL intends to address these market concerns.

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 in Portugal, and the development of its replication process for other countries and markets.

In the context of software development, a framework 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 be used and analysed are associated with the protection against cyberattacks and the security of information across its entire lifecycle. They will be validated by National Institute of Medical Emergency (INEM).

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:

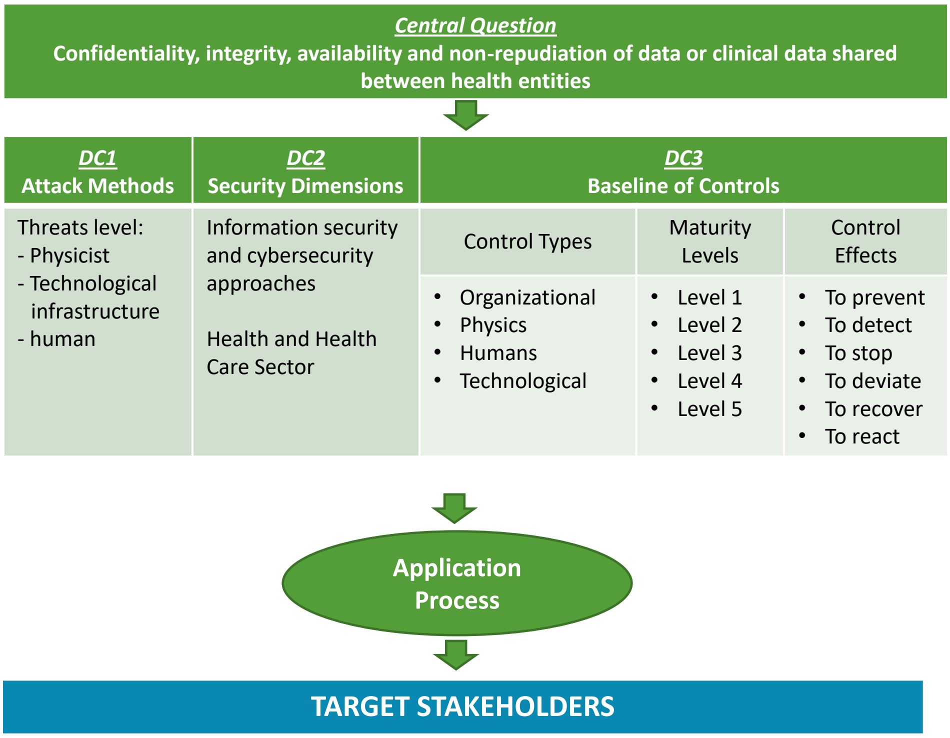


Figure 1 – Framework Configuration

Use Cases

Objectives of the Framework

(1) **Use Case INEM:** Protect the application bubble with clinical information installed in each entity.

(2) **Use Case Medical Equipment**: Improve safety of medical signal monitoring devices.

(3) **Use Case Shared:** Ensuring trust between entities that plan to share information, ensuring the same level of maturity, by definition of the roadmap to be followed at the HISC4All level for the entity at a lower level. Future vision: sharing of information between INEM and health entities.

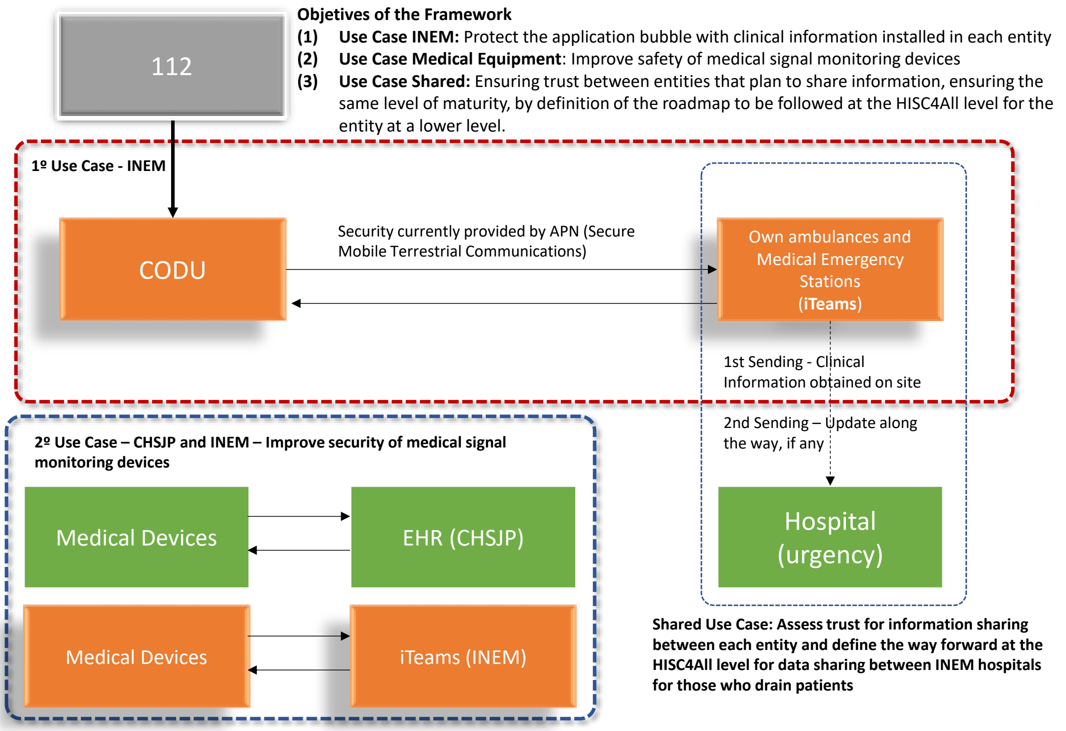
Use Case I (INEM): Ensure the Cybersecurity and Information Security of the applications in which clinical information is stored, processed or transmitted, as well as the systems that directly support their operation.

Use Case II (CHUSJ and INEM): Ensure the Cybersecurity and Information Security of medical devices by monitoring the signals and the surrounding environment where they are inserted and used.

Use Case III: Ensure the same level of Cybersecurity and Information Security maturity 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).

HISC4ALL shall define security levels / control baselines 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.

The following presentation intends to describe the use cases, trying to reflect their use in specifying high-level functional and non-functional requirements, in the dimension to be applied with the development of the project:



Objetives of the Framework

(1) **Use Case INEM:** Protect the application bubble with clinical information installed in each entity

(2) **Use Case Medical Equipment**: Improve safety of medical signal monitoring devices

(3) **Use Case Shared:** Ensuring trust between entities that plan to share information, ensuring the same level of maturity, by definition of the roadmap to be followed at the HISC4All level for the entity at a lower level.

112
1º Use Case - INEM
CODU
Security currently provided by APN (Secure Mobile Terrestrial Communications)
Own ambulances and Medical Emergency Stations (iTeams)
1st Sending - Clinical Information obtained on site
2nd Sending – Update along the way, if any
Hospital (urgency)
2º Use Case – CHSJP and INEM – Improve security of medical signal monitoring devices
Medical Devices
EHR (CHSJP)
Medical Devices
iTeams (INEM)

Shared Use Case: Assess trust for information sharing between each entity and define the way forward at the HISC4All level for data sharing between INEM hospitals for those who drain patients

Figure 2 – Use Cases: Project Vision

Alignment with the Activities described in the Call document

The action to be developed with the Project HISC4ALL will support cybersecurity resilience in healthcare and health institutions, following the stress over the recent years, especially intensified by the COVID-19 crisis, in view of limiting the damage of safety-critical cybersecurity incidents which have affected hospitals and health services providers.

The project, integrated in digital transformation in European Union, where cybersecurity plays an important role, addresses the following main areas:

- Implementation of objectives and requirements under the NIS Directive in relation to the health sector.
- Adoption in healthcare and health institutions, and in particular SMEs, of tools, methods, organisational and management practices dedicated to cybersecurity. Also, the exchange of information between peers.
- Cybersecurity education, awareness and skills development in healthcare and health institutions.

The Project intends to create a Market Solution to incorporate in the market Products, Services, Knowledge, Training, Awareness raising and Information Sharing, in the area of the Cybersecurity in the Healthcare Institutions and Health Sector.

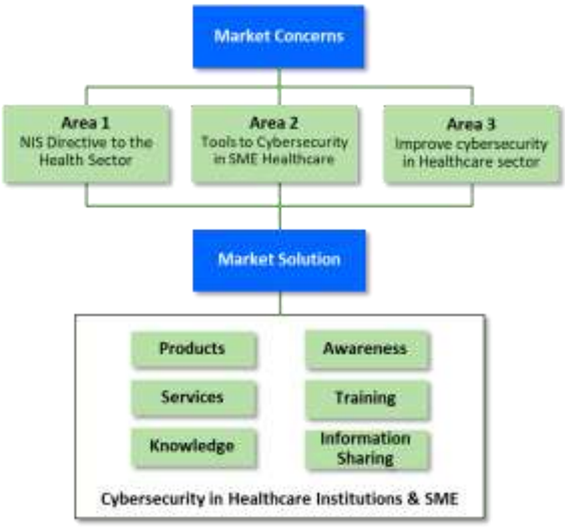

Market Concerns
Area 1
NIS Directive to the Health Sector
Area 2
Tools to Cybersecurity in SME Healthcare
Area 3
Improve cybersecurity in Healthcare sector
Market Solution
Products
Awareness
Services
Training
Knowledge
Information Sharing
Cybersecurity in Healthcare Institutions & SME

Figure 2 – Use Cases: Project Vision

The practical applicability of creating the Framework, both for the Information Security and Cybersecurity in Health market, for SMEs that interact in this market, and for society in general, will be as follows:

- **Products** that can be placed on the market later
  - Information security and cybersecurity assessment product;
  - Product that allows automating the design of a road map of implementation activities and control improvement, based on the assessment results and in accordance with the intended security baseline and the maturity levels of the associated controls.
- **Services** that can be developed/performed after the framework is developed
  - ➢ The above-mentioned product support implementation and market functioning services.
- **Skills** that could be added to the SME market as a result of designing the framework
  - ➢ Best practices in the implementation of controls associated with the framework that supports the aforementioned products
- **Training** areas that will need to be created

   - Training on the framework; Training on the implementation process; Training on the operation

- **Awareness-raising** actions on the topic of information security/cybersecurity can be developed following the creation of the framework
   - Awareness actions at 3 levels: Board of Directors; Intermediate frames (C level); users
- **Information sharing** actions that can be implemented
   - Lessons learned resulting from the application of the framework

General Objective from the Scope

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

- 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, of tools, methods, organisational 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.*

Promoters

- Instituto Nacional de Emergência Médica (INEM) – Public Institution from the Ministry of Health, responsible for the Integrated Medical Emergency System.
- PAHLDATA – Private SME, Health Sector Solutions Provider.
- CHUSJ – Centro Hospitalar Universitário de São João, Porto – Public sector hospital, integrated in the Portuguese public health system, reporting to the Ministry of Health of the Portuguese Government.

Target *Stakeholders*

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

Solution to Support to Cybersecurity in the Health Sector

The project will, therefore, **design of a common and shared Information Security and Cybersecurity Framework** for the health sector, and its application process, promoted by a **public-private Consortium**, including a public medical emergency service, a public university hospital and a private SME specialized in the health sector and healthcare institutions.

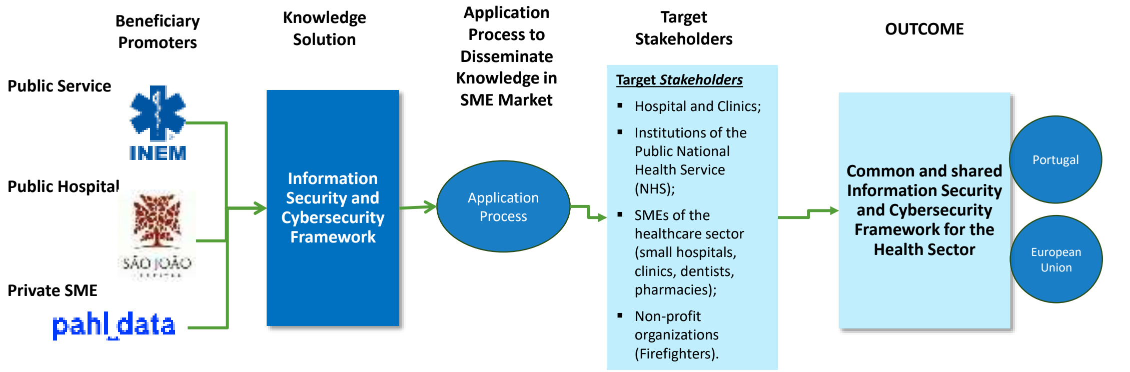

Beneficiary Promoters
Knowledge Solution
Application Process to Disseminate Knowledge in SME Market
Target Stakeholders
OUTCOME
Public Service
INEM
Public Hospital
SÃO JOÃO
Private SME
pahl data
Information Security and Cybersecurity Framework
Application Process
Target Stakeholders
Hospital and Clinics;
Institutions of the Public National Health Service (NHS);
SMEs of the healthcare sector (small hospitals, clinics, dentists, pharmacies);
Non-profit organizations (Firefighters).
Common and shared Information Security and Cybersecurity Framework for the Health Sector
Portugal
European Union

Figure 3 – Introduction of the Framework in the Market

Activities of the Project

Project HISC4ALL will be developed in 4 phases and in 22 activities, as presented bellow and developed through the Work Packages presented in point 4.

Phase I. 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.

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)

Phase II. MARKET TEST

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

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

Activity 7. Perform the Interviews: Focus Group (Uses Cases and requirements specification).

Activity 8. Communication & Dissemination Plan

Activity 9. Design of the Security Controls Framework (v2.0): baselines by security dimension and control maturity levels.

Activity 10. Training, Awareness and Training Program in the implementation and operation of the Framework (v1.0).

Activity 11. Framework Support Application

Activity 12. Website

Activity 13. Market Self-Assessment (II)

Phase III. CONCEPTION & APPLICATION

Activity 14. Design of the framework application process.

Activity 15. Application of the framework to health entities (Action Research – a single cycle) (PoC – Proof-of-Concept)

Activity 16. Collection of lessons learned.

Activity 17. Design of the security controls framework (v3.0): security dimensions and controls by dimension.

Activity 18. HISC4ALL update

Activity 19. Market Validation + Website

PHASE IV. DISSEMINATION

Activity 20. Availability of the HISC4All Tool

Activity 21. Communication & Dissemination Plan + Website

Activity 22. Implementation Plan

Activity 23. Final Report

1.2 Contribution to long-term policy objectives, policies and strategies — Synergies

Contribution to long-term policy objectives, policies and strategies — Synergies

Describe how the project contributes to long-term policy objectives of the call's domain/area and to the relevant policies and strategies, and how it is based on a sound needs analysis in line with the activities at European and national level.

What challenge does the project aim to address?

The objectives should be specific, measurable, achievable, relevant and time-bound within the duration of the project.

Project contribution to long-term policy objectives of the call areas and to relevant policies and strategies

In early 2020, the world's digital economy has grown 2,5 times faster than global GDP over the past 15 years. The **rapid development of digital technologies** also brings new security challenges, in a time where all sectors are undergoing digital transformation.

New technologies like cloud, the Internet of Things (IoT), and artificial intelligence (AI) are spreading. All of these mean that **cyber security risks are rising**. If the world wants to benefit from the expansionary economic impact of ICT, maintaining secure ICT environment is very important. The health and the healthcare institutions are facing some challenges, including because of the stresses provoked by the pandemic situation of COVID-19.

The whole world is really aware of how important cybersecurity is for ensuring trust in the digital world. Cybersecurity involves many elements and stakeholders. An all-industries, full-society approach to collaboration is essential to enhancing systematic cyber security governance for everyone.

Today, ICT is driving tremendous socioeconomic development. Meanwhile, cyber-attacks are increasing rapidly.

To address these challenges, the **Digital Europe Programme** provides funding for projects in five crucial areas:

- supercomputing

- artificial intelligence
- **cybersecurity**
- advanced digital skills
- ensuring the wide use of digital technologies across the economy and society.

As presented itself, the programme is designed to **bridge the gap between digital technology research and market deployment**, aiming to benefit Europe's citizens and businesses, especially SMEs.

Investment under the Digital Europe Programme supports the European Union’s twin objectives of a green transition and digital transformation while strengthening the Union’s resilience and digital sovereignty.

The HISC4ALL project is fully embarked in this long-rum Europe Strategy.

The long-term contribution involves the design of a common and shared framework for the health sector in Portugal, later released to other European countries, which makes it possible to assess, design and implement the most relevant controls for the defined uses cases (requirements).

The design of the project will be based on a conceptual framework fundamentally supported by a set of concepts already defined in academic subjects related to Information Security, Information Systems and Cybersecurity (e.g. Computer Network Security, Software Security, Cryptography, Risk Management) and/or national or international standards (e.g. ISO/IEC, NIST).

In this way, the focus of the project is on clearly promoting the objectives defined in the 3 intervention areas defined in the Call for Proposal DIGITAL-2022-CYBER-02-SUPPORTHEALTH - Support To Cybersecurity In The Health Sector:

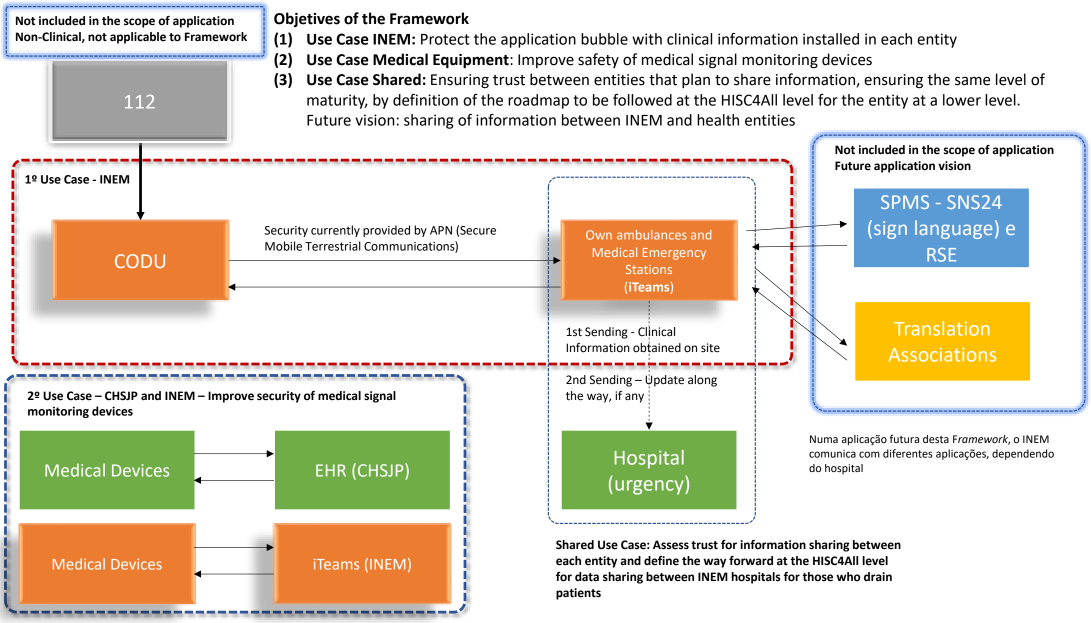
- Implementation of actions among the SME market under the NIS Directive in relation to the health sector.
- Implement in the healthcare and health institutions, and in particular SMEs, of tools, methods, organizational and management practices dedicated to cybersecurity, as well promoting the exchange of information within the sector.
- Promote the cybersecurity education, awareness and skills development in healthcare and health institutions.

<u>How the project is based in sound needs analysis in line with European and national level</u>

The project is strongly supported by the development of the Use Cases, mentioned in the previous point.

As the project is based on solid needs analysis, in line with European and national levels, it is intended to be aligned with the international policies, guidelines and standards (ENISA, NIS) and national (CNCS and health), as well with the defined uses cases.

The following diagram is an example of how the various Use Cases will work and interact with each other, also explaining the three main objectives of the Framework associated with them, considering the future evolution.



Objetives of the Framework

(1) **Use Case INEM:** Protect the application bubble with clinical information installed in each entity

(2) **Use Case Medical Equipment**: Improve safety of medical signal monitoring devices

(3) **Use Case Shared:** Ensuring trust between entities that plan to share information, ensuring the same level of maturity, by definition of the roadmap to be followed at the HISC4All level for the entity at a lower level. Future vision: sharing of information between INEM and health entities

Numa aplicação futura desta *Framework*, o INEM comunica com diferentes aplicações, dependendo do hospital

Shared Use Case: Assess trust for information sharing between each entity and define the way forward at the HISC4All level for data sharing between INEM hospitals for those who drain patients

Not included in the scope of application
Non-Clinical, not applicable to Framework
112
1º Use Case - INEM
CODU
Security currently provided by APN (Secure Mobile Terrestrial Communications)
Own ambulances and Medical Emergency Stations (iTeams)
1st Sending - Clinical Information obtained on site
2nd Sending – Update along the way, if any
Hospital (urgency)
Not included in the scope of application
Future application vision
SPMS - SNS24 (sign language) e RSE
Translation Associations
2º Use Case – CHSJP and INEM – Improve security of medical signal monitoring devices
Medical Devices
EHR (CHSJP)
Medical Devices
iTeams (INEM)

Figure 4 – Use Cases: Project Vision

Challenges the project aim to address

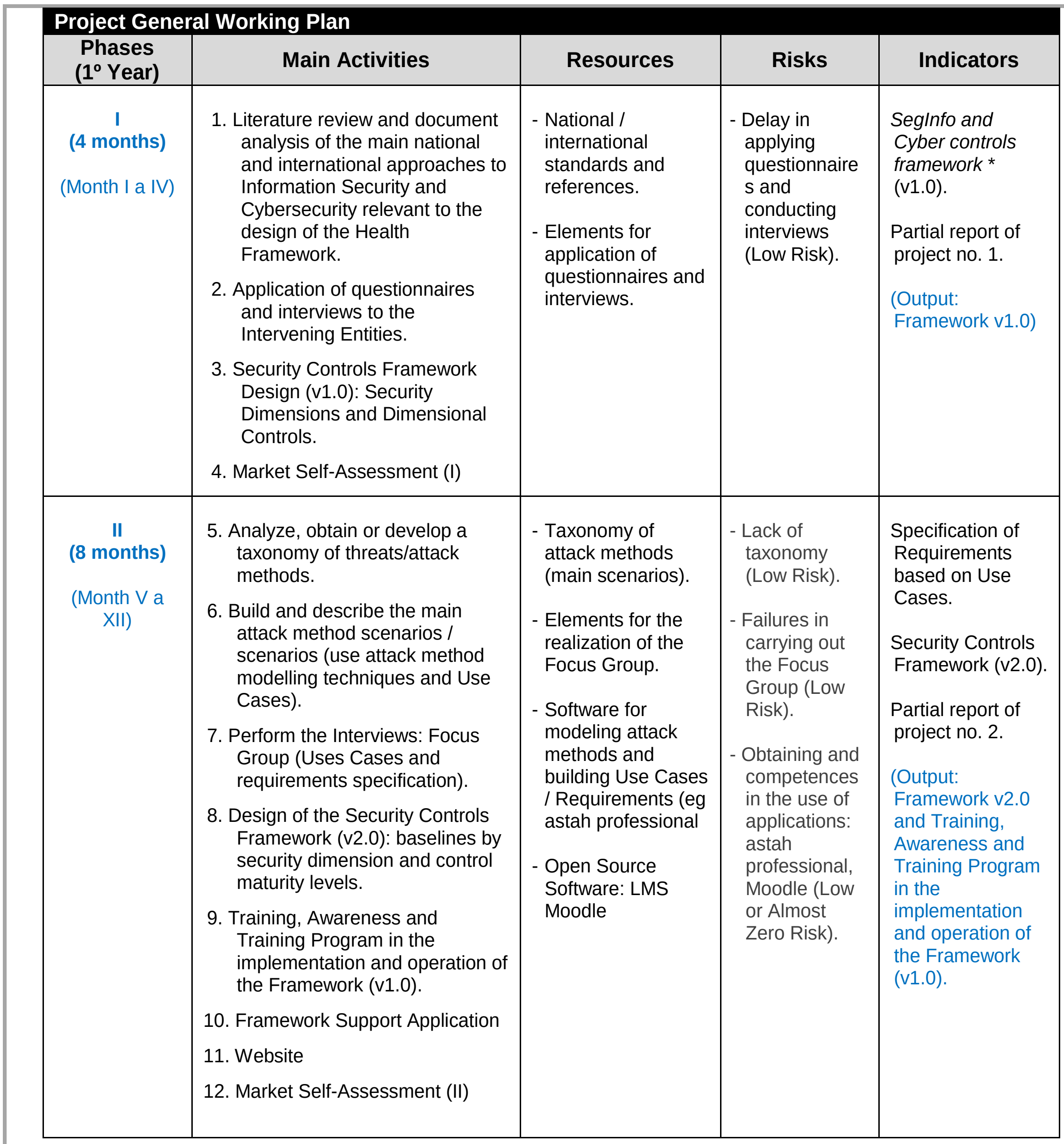
There are five challenges to be met with the implementation of the HISC4ALL project, in line with the European Union's long-term policy objectives, policies and strategies:

1. Design of the Information Security and Cybersecurity framework;
2. Design and modulation of the framework implementation process;
3. Design and modulation of the framework's operating process;
4. Design of the training, awareness and training programme;
5. Development of the application that incorporates the knowledge of the previous points.

Objectives specific, measurable, achievable, relevant and time-bound within the duration of the project

The work plan designed to carry out the project, discriminated at point 4 of the application form, seeks to accurately define all objectives Specific, Measurable, Achievable, Relevant and Time-Bound Within the Duration of the Project, or meet all proposed. It is presented summarily in the following table, with the indication of its main phases and activities, being the detailed planning later through the Critical Path Method (CPM).

The main resources needed for their realization, the risks and, finally, the indicators of success, that is, the fundamental objectives to be achieved in different phases and activities (delivered) are also referenced.



Project General Working Plan				
Phases (1º Year)	**Main Activities**	**Resources**	**Risks**	**Indicators**
I **(4 months)** (Month I a IV)	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. 2. Application of questionnaires and interviews to the Intervening Entities. 3. Security Controls Framework Design (v1.0): Security Dimensions and Dimensional Controls. 4. Market Self-Assessment (I)	- National / international standards and references. - Elements for application of questionnaires and interviews.	- Delay in applying questionnaires and conducting interviews (Low Risk).	*SegInfo and Cyber controls framework ** (v1.0). Partial report of project no. 1. (Output: Framework v1.0)
II **(8 months)** (Month V a XII)	5. Analyze, obtain or develop a taxonomy of threats/attack methods. 6. Build and describe the main attack method scenarios / scenarios (use attack method modelling techniques and Use Cases). 7. Perform the Interviews: Focus Group (Uses Cases and requirements specification). 8. Design of the Security Controls Framework (v2.0): baselines by security dimension and control maturity levels. 9. Training, Awareness and Training Program in the implementation and operation of the Framework (v1.0). 10. Framework Support Application 11. Website 12. Market Self-Assessment (II)	- Taxonomy of attack methods (main scenarios). - Elements for the realization of the Focus Group. - Software for modeling attack methods and building Use Cases / Requirements (eg astah professional - Open Source Software: LMS Moodle	- Lack of taxonomy (Low Risk). - Failures in carrying out the Focus Group (Low Risk). - Obtaining and competences in the use of applications: astah professional, Moodle (Low or Almost Zero Risk).	Specification of Requirements based on Use Cases. Security Controls Framework (v2.0). Partial report of project no. 2. (Output: Framework v2.0 and Training, Awareness and Training Program in the implementation and operation of the Framework (v1.0).

Figure 5 – Project General Working Plan – First Year

Project General Working Plan (cont.)

Phases (2º Year)	Main Activities	Resources	Risks	Indicators
III **(10 months)** (Month I a X)	13. Design of the framework application process. 14. Application of the framework to health entities (Action Research – a single cycle) 15. Collection of lessons learned. 16. Design of the security controls framework (v3.0): security dimensions and controls by dimension. 17. HISC4ALL update 18. Market Validation + Website	- International standards. - Entities / Organizations to apply the framework *(proof of concept: one baseline per dimension of the framework)*	- Availability of Entities /Organizations to apply the framework (Low Risk).	*Framework Application Process (v1.0).* *Security Controls Framework (v3.0).* *Partial report of project no. 3.* *(Outputs: Framework v3.0 and Application Process)*
IV **(2 months)** (Month XI e XII)	19. Availability of the HISC4All Tool 20. Communication & Dissemination Plan + Website 21. Implementation Plan 22. Final Report	-	-	*SegInfo Framework and Cybersecurity.* *Final Framework* *Application Process* Implementation Plan Communication & Dissemination Plan Final Project Report. (Outputs: Framework v3.0, Application Process, Operation Process and Final Training, Awareness and Training Program for the implementation and Operation of the Framework).

Figure 6 – Project General Working Plan – Second Year

1.3 Digital technology supply chain

Digital technology supply chain

Explain to what extent the project would reinforce and secure the digital technology supply chain in the EU.

⚠ *This criterion might not be applicable to all topics — for details refer to the Call document.*

What extent the project would reinforce and secure the digital technology supply chain in the EU

This project addresses a weakness detected in the interconnections between national health entities, allowing, after its implementation, to reinforce the information security and cybersecurity of the systems that share clinical data, thus ensuring the entire security of the chain.

This is a problem across EU countries, thus opening up the opportunity to provide new digital services across borders, ensuring a high level of protection of clinical data (personal and sensitive).

2. IMPLEMENTATION

2.1 Maturity

Maturity

Explain the maturity of the project, i.e. the state of preparation and the readiness to start the implementation of the proposed activities.

Maturity of the project - the state of preparation and the readiness to start the implementation of the proposed activities

An initial literature review was performed, based on academic publications. There are elements in the team with high academic and professional qualifications to lead and actively collaborate in the design, planning, development, operation and training, activities inherent to the project to be developed.

The team has solid, consistent and up-to-date knowledge of the various national and international approaches to cybersecurity and information security (previous examples; ISO/IEC 27001, ISO/IEC 27032, NIST 800-53, NIST Framework Cybersecurity), as well as some of the most relevant certifications in these domains (examples: CISSP, CISM).

A prospective diagnosis of the entities involved in the project was carried out, which is reflected in the Use Cases presented.

Consequently, the team created will allow for a short and medium term response to the challenges of this project, according to the time line presented.

2.2 Implementation plan and efficient use of resources

Implementation plan

Show that the implementation work plan is sound by explaining the rationale behind the proposed work packages and how they contribute to achieve the objectives of the project.

Explain the coherence between the objectives, activities, planned resources and project management processes.

Show how the project integrates, builds on and follows up on any pre-existing work or EU funded projects. Provide details (including architecture and deliverables) about pre-existing technical solutions.

Implementation work plan sound by explaining the rationale behind the proposed work packages and how they contribute to achieve the objectives of the project

As presented, the aim is to *create a new framework to assess the level of maturity of the different actors in the health sector involved in sharing data and information with and within each other. The purpose is to ensure that these exchanges take place between entities that meet certain minimum-security requirements and, to this end, comply with the highest levels of the maturity model to be developed*.

Design and Planning

The design and planning of Information Security and Cybersecurity must be carried out taking into account the main attack vectors of an adversary and risk management, as already mentioned, and must ensure a rigorous attribution of responsibilities to the various levels of management of the organization.

The structuring of the Information Security and Cybersecurity dimensions in a Controls Framework must be guided by the attack vectors, and must be modelable and scalable to allow the integration of the controls suggested by various relevant references, of which, after document analysis, the standard ISO/IEC 27001, NIST 800-53, CISSP certification, the twenty cybersecurity controls suggested by the Center for Internet Security, the NIST cybersecurity framework, among others.

This framework must also reference control baselines and there must be maturity levels associated with the controls.

However, it should be taken into account that Information Security and Cybersecurity at the level of organizations is a Wicked Problem, taking into account the criteria for accepting a Wicked Problem, of which the following stand out: (i) there is no definitive formulation of the problem; (ii) the solutions to the problem are not true or false, but better or worse; (iii) there is no immediate and final test of the solution found to the problem; (iv) each problem is unique; (v) the causes of a problem can be explained in several ways, consequently the choice of explanation of the problem determines the nature of the resolution of the same.

Information Security and Cybersecurity Principles

The following can be considered as some of the main ones to be applied in the scope of Information Security and Cybersecurity:

(1) **Defence in depth**: suggests the need for an Organization to have its security controls implemented in depth, and the effects to be obtained with the application of security controls (e.g., prevent, detect, detain).

(2) **Need to Know**: the application of this principle seeks to ensure that only people/Systems who need information to carry out their activities can have access to it.

(3) **Minimum Privilege**: its application seeks to ensure that people who have access to information can only perform a set of previously authorized minimum actions.

(4) **Ease of Intrusion**: this principle implies that all possible scenarios of intrusion into a System must be considered, hence the importance of attack taxonomies and modelling techniques.

(5) **Adequate Protection**: a System must be protected according to its value. This protection is fundamentally guided by the information security properties, that is, by confidentiality, integrity, availability. One approach that organizations can use to identify protection measures to implement is “Risk Management” combined with baselines of security controls.

(6) **Effectiveness in Protection**: this principle refers to the need and importance of guaranteeing the effectiveness and efficiency of the protection measures to be implemented by the Organization to mitigate an attack method. Not forgetting, of course, the resources used in the solution, its costs, the time required and its complexity.

(7) **Weakest Link**: means that the security level of a System (e.g., Organization) reflects its weakest link. In order to have a level stronger than its weakest link, it is necessary that the controls applied take into account the security principles mentioned above and that the Organization implements a security architecture where the various security dimensions (e.g., organizational, physical, human and technology) are interconnected

Cybersecurity Approaches

It is essential that the proposed framework integrates the controls recommended by some of the main cybersecurity references, which are considered from the outset: (i) the international standard ISO/IEC 27032 (2012) of good cybersecurity practices; (ii) the twenty controls recommended by the Center for Internet Security - CIS (CIS, 2018) which are grouped into three families or classes of controls (“Basic – Foundational – Organizational”); (iii) and the “Framework for Improving Critical Infrastructure Cybersecurity” (NIST Cybersecurity, 2014) from NIST.

Control Effects

As for the effects of controls, they may have the following objectives:

(1) **Prevent**: anticipate. Within the scope of Information Security and Cybersecurity, it consists of preparing and, if possible, preventing the occurrence of a threat / Attack Method (e.g., executing an Awareness and Training Plan).

(2) **Detect**: reveal the existence of what is hidden. It consists of revealing the threat / Attack Method that is occurring or that has already occurred (e.g. Implement IDS / IPS).

(3) **Stop**: to stop, suspend, interrupt. It consists of stopping or delaying the threat / Attack Method that is occurring or its possible effects (e.g., Implement Firewall).

(4) **Deflect**: move away, change direction. It consists of directing the threat / Attack Method that is occurring to a system that, if hit, does not impact the Organization (e.g., Implement Honeypots).

(5) **Recover**: restore, return to initial state. It consists of recovering from the occurrence and effects of the threat / Attack Method (e.g., Restore Information Backup Copies, i.e., Backups).

(6) **React**: respond in a certain way to an action. It consists of executing a set of actions in response to the occurrence and effects of the threat / Method of Attack (e.g., Execute the Disaster Recovery Plan).

Risk Management

The theme of risk management is central and undoubtedly a common denominator: (i) in the design, implementation and operation of Information Security Management Systems (eg ISO/IEC 27001, ISO/IEC 27005); (ii) in Cybersecurity (eg ISO/IEC 27032); (iii) in the preparation of business continuity plans (eg ISO/IEC 22301); (iv) and also in the protection of personal data (eg ISO/IEC 27701) at the level of organizations.

As it turns out:

(1) The international standard ISO/IEC 27001 (2013) complemented with ISO/IEC 27005 (2018) in the scope of Information Security management, explicitly states that an Organization must carry out risk assessments at planned intervals or when changes occur and must keep this information documented. You must also plan and implement a risk treatment plan.

(2) Within the scope of Cybersecurity, the ISO/IEC 27032 (2012) standard is also clear in referencing and suggesting the use of the ISO/IEC 27005 and ISO/IEC 31000 standards for the assessment and treatment of their risks.

(3) Also in the implementation of Business Continuity Management Systems it is critical that the organization establish, implement and maintain a formal and documented process for business impact analysis and risk assessment (ISO/IEC 22301, 2019).

(4) Finally, within the scope of Privacy Management Systems, one of the fundamental aspects in the security of personal data is the ability to apply the appropriate technical and organizational measures to ensure a level of security adequate to the risk (Article 32 of the General Data Protection Regulation - GDPR). These measures are referenced and suggested in ISO/IEC 27701 (2019), an international standard that extends ISO/IEC 27001.

Taking into account the importance of Risk Management, this must be considered as a fundamental System in the process of applying the Information Security and Cybersecurity Framework.

Research Methodology (Design Science)

The design of the Framework predominantly follows an interpretative, qualitative and inductive epistemological orientation, which uses document analysis, the application of questionnaires and interviews with the intervening / participating health entities as the main information collection techniques, and as research methods the Focus Group and Action Research. It will essentially be a Design Science and Applied Science project executed according to scientific guidelines and rules defined and accepted by the scientific communities of Information Systems and Software Engineering.

Theoretical Support

Its design will be based on a conceptual framework fundamentally supported by a set of concepts already defined in academic subjects related to Information Security, Information Systems and Cybersecurity (eg Computer Network Security, Software Security, Cryptography, Risk Management) and/or national or international standards (eg ISO / IEC, NIST).

Initial Literature Review

Taking into account the literature review already carried out and the experience of the consortium members, the following main points are previously considered as guidance for the design of the Framework (Figure 7) below:

(1) The structuring of the Framework's Information Security and Cybersecurity dimensions must be guided by the main attack vectors. Simultaneously, each security dimension (eg Organizational, Physical, Human, Technological) must have associated control baselines (e.g. 1 to 3; 1 to 5; 1 to 7) with transition criteria identified and rationale specified.

(2) The implementation of security controls in any organization should follow the set of most relevant Information Security and Cybersecurity approaches and references (eg ISO/IEC 27001, ISO/IEC 27002, NIST 800-53, National Reference Framework for Cybersecurity - Portugal, Cybersecurity Frameworks) and complemented with Risk Management (eg ISO 31000, ISO/IEC 27005, NIST 800-30, NISTIR 8286 A, HIMSS - INFRAM).

(3) Security controls are fundamentally organizational, physical, human and technological (eg indicated by the international standard ISO / IEC 27002), must have associated maturity levels from one to five (eg adaptation of the CMMI), have associated more effects (eg prevent, detect, deter, divert and recover) and associated metric(s) / Indicator(s).

(4) The Framework concept of implementation process will be guided by the following five main phases (Figure 8) below:

(i) initial diagnosis ("as is");

(ii) design and instantiation of controls in the reality of the Organization / Entity, taking into account the intended selected baseline and the maturity levels of the associated controls;

(iii) implementation of controls (eg, policies, plans, processes, procedures, technology);

(iv) monitoring and auditing (metrics and indicators);

(v) and continuous improvement (PDCA Model).

(5) Project management will be carried out taking into account the preferential use of the PM2 methodology (Project Management Methodology – current version 3.0.1) developed and made available by the European Union or the PMBok Practices from Project Management Institute - PMI.

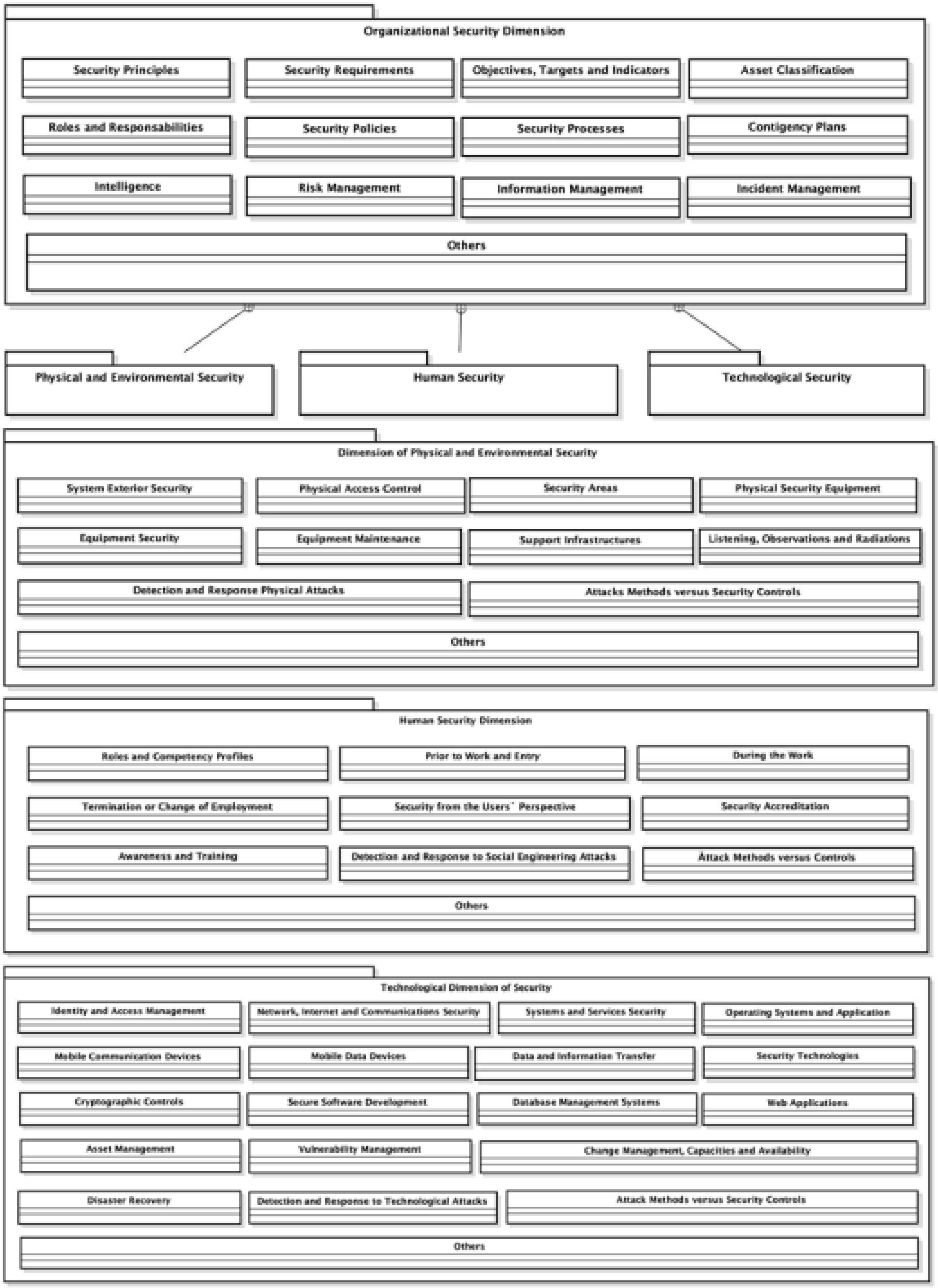

Organizational Security Dimension
Security Principles
Security Requirements
Objectives, Targets and Indicators
Asset Classification
Roles and Responsabilities
Security Policies
Security Processes
Contigency Plans
Intelligence
Risk Management
Information Management
Incident Management
Others
Physical and Environmental Security
Human Security
Technological Security
Dimension of Physical and Environmental Security
System Exterior Security
Physical Access Control
Security Areas
Physical Security Equipment
Equipment Security
Equipment Maintenance
Support Infrastructures
Listening, Observations and Radiations
Detection and Response Physical Attacks
Attacks Methods versus Security Controls
Others
Human Security Dimension
Roles and Competency Profiles
Prior to Work and Entry
During the Work
Termination or Change of Employment
Security from the Users´ Perspective
Security Accreditation
Awareness and Training
Detection and Response to Social Engineering Attacks
Àttack Methods versus Controls
Others
Technological Dimension of Security
Identity and Access Management
Network, Internet and Communications Security
Systems and Services Security
Operating Systems and Application
Mobile Communication Devices
Mobile Data Devices
Data and Information Transfer
Security Technologies
Cryptographic Controls
Secure Software Development
Database Management Systems
Web Applications
Asset Management
Vulnerability Management
Change Management, Capacities and Availability
Disaster Recovery
Detection and Response to Technological Attacks
Attack Methods versus Security Controls
Others

Figure 7 – Information Security and Cybersecurity Framework (Overview)

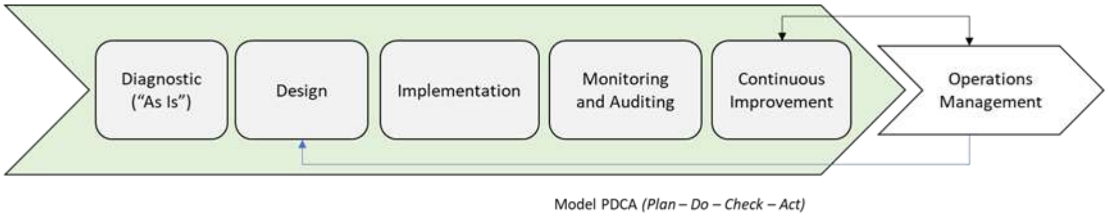


Figure 8 – General Framework Design, Implementation and Operation Process

Capacity & Training

As stated by Peltier (2005), an effective Information Security System (and Cybersecurity) cannot be implemented without promoting a training, awareness and training program for the Organization's employees, which must address the policies, procedures and implemented tools. The implementation and operation of the Framework also needs to be associated with an Information Security and Cybersecurity training program.

Program, in which the development of appealing content for training and awareness-raising actions (e.g., videos) must be ensured. These should allow greater realism, employee participation and facilitate the “passing of the message”, making content available, whenever possible, through E-learning Platforms (e.g., LMS Moodle).

Training, awareness and training requires, in order to make the actions more effective, that trainers are aware of the importance of the main theories of learning (Learning Psychology) and the most recent discoveries in Neuroscience (e.g., Memory, Emotions, Motivation Mechanisms). This will certainly influence the way in which training should be carried out and its influence on the learning of those involved. A close link between practical experience and theoretical knowledge should be sought whenever possible during the construction and communication of the message.

Another important aspect is the sharing of experiences, i.e., lessons learned between employees. One of the ways, among others, to carry out this sharing is to have an automated process that makes it possible to make Case Studies available to those who need to know them according to their activities and whose main objective is to avoid the repetition of the errors identified in the Case. In this way, it contributes to Knowledge Management in the area of Information Security and Cybersecurity in the health sector and in the sharing of experience between the various organizations / entities.

After designing the Framework and the associated implementation and operation processes, a general education, awareness and training program will be designed with five phases (Figure 9) and with the main objective of ensuring the efficient and effective implementation and operation of the Framework.

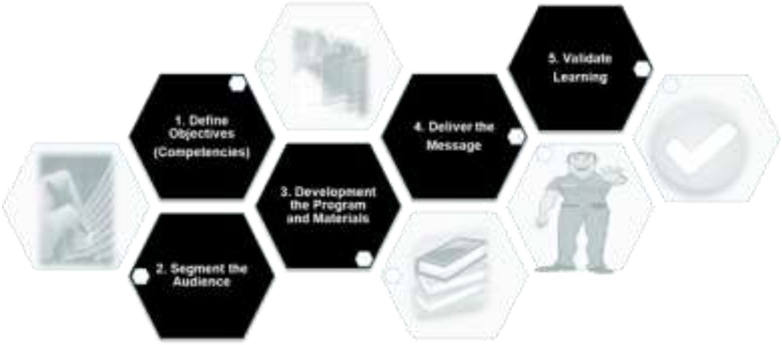

1. Define Objectives (Competencies)
2. Segment the Audience
3. Development the Program and Materials
4. Deliver the Message
5. Validate Learning

Figure 9 – Training, Awareness and Training Program

Coherence between the objectives, activities, planned resources and project management processes

Activities of the Project

Project HISC4ALL will be developed in 4 phases and in 22 activities, as presented in the following table and developed through the Work Packages presented in point 4.

Phase I. 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 se ideas about contend of the framework, to star receiving feedback and information about the needs and expectations.

Activity 3. Security Controls Framework Design (v1.0): Security Dimensions and Dimensional Controls.

Strat 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 firs version of the draft framework conceived. First with INEM, an after near the other beneficiary stakeholders of the market. Make a database of the testing 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. 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 scenarios / scenarios (use attack method modelling techniques and Use Cases).

Build and scenarios.

Activity 7. Perform the Interviews: Focus Group (Uses Cases and requirements specification).

With a guide and oriented results approach, focused in collecting comments and improving suggestions.

Activity 8. Develop a Communication & Dissemination Plan.

Develop a communication and dissemination plan, to promote the communications of the activities developed by the project and the activitis to disseminate the results after the project ending.

Activity 9. Design of the Security Controls Framework (v2.0): baselines by security dimension and control maturity levels.

Continue to develop the HISC4ALL.

Activity 10. 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 11. Framework Support Application

Conceive the framework support application.

Activity 12. Website

Develop a first version of the website.

Activity 13. Market Self Assessment (II)

Apply a market test of the second version of the framework to the selected stakeholders defined.

Phase III. CONCEPTION & APPLICATION

Activity 14. Design of the framework application process.

Conceive the framework application process.

Activity 15. Application of the framework to health entities (Action Research – a single cycle)

Presenting the final version to a set of healthcare institutions to validate.

Activity 16. Collection of lessons learned.

Register and incorporate the final remarks/suggestions.

Activity 17. Design of the security controls framework (v3.0): security dimensions and controls by dimension.

Activity 18. HISC4ALL update

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

Activity 19. Market Validation + Website

Make a final validation and upgrade of the website.

PHASE IV. DISSEMINATION

Activity 20. 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 21. 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.

Activity 22. Implementation Plan

Develop a plan for the development of future market and technical applications of the created framework, aiming to improve of the processes 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.

Activity 23. Final Report

Develop the project final report, 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

Organization of Activities

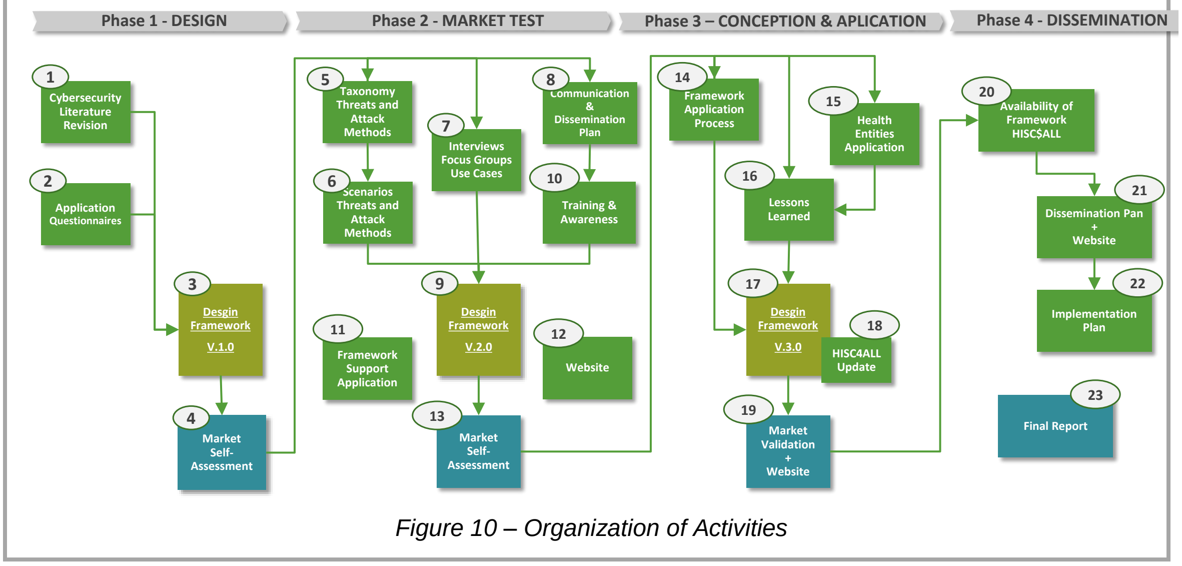

Phase 1 - DESIGN
Phase 2 - MARKET TEST
Phase 3 – CONCEPTION & APLICATION
Phase 4 - DISSEMINATION
1
Cybersecurity Literature Revision
2
Application Questionnaires
3
Desgin Framework V.1.0
4
Market Self-Assessment
5
Taxonomy Threats and Attack Methods
6
Scenarios Threats and Attack Methods
7
Interviews Focus Groups Use Cases
8
Communication & Dissemination Plan
9
Desgin Framework V.2.0
10
Training & Awareness
11
Framework Support Application
12
Website
13
Market Self-Assessment
14
Framework Application Process
15
Health Entities Application
16
Lessons Learned
17
Desgin Framework V.3.0
18
HISC4ALL Update
19
Market Validation + Website
20
Availability of Framework HISC$ALL
21
Dissemination Pan + Website
22
Implementation Plan
23
Final Report

Figure 10 – Organization of Activities

Project management, quality assurance and monitoring and evaluation strategy

Describe the measures planned to ensure that the project implementation is of high quality and completed in time.

Describe the methods to ensure good quality of monitoring, planning and control activities.

Describe the evaluation methods and indicators (quantitative and qualitative) to monitor and verify the outreach and coverage of the activities and results. The indicators proposed to measure progress should be specific, measurable, achievable, relevant and time-bound.

Project management

To ensure *that the project implementation is of high quality and completed in time, it will be used the following project management models.*

1. PMBok / PMI

It is the main framework to be used to manage the HISC4ALL project, based on PMBok/PMI practices.

The PMBOK is a guide to good practices, guidelines and definitions related to project management. The purpose of the PMBOK is to clarify understanding of the various areas of knowledge, such as: Scope, Budgeting/Costs, Schedule, Quality, Resources, Communication, Procurement and Stakeholders. These competences are the set of areas that help in the management of a project.

2. PDCA Model (successive improvements)

As already mentioned, in addition to the main Framework, the implementation process will be guided by the following successive improvement phases of the PDCA model (successive upgrades), on each phase of the 4 Work Packages:

- Plan – Planning:
- Do – Implementing, running;
- Check – Auditing, verification;
- Act – Acting.

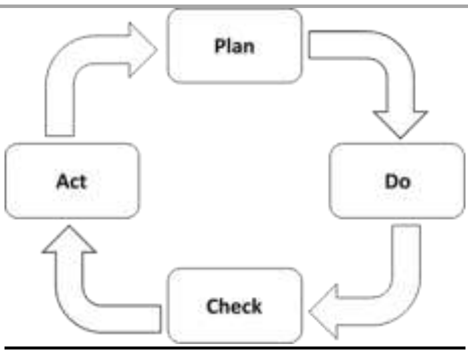


Figure 11 – Project Management Model

3. Risk Management Model

The risk management model adopted will be as follows:

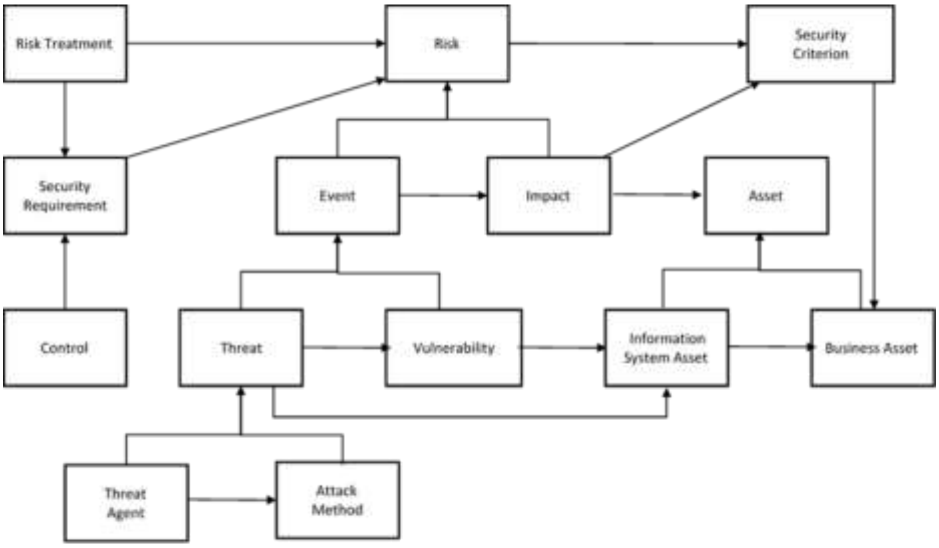


Figure 12 – Risk Management Model

4. Quality Assurance

The methods to ensure good quality of monitoring, planning and control activities, include:

- Apply the management models identified;
- Apply the consortium management model defined;
- Continuous monitoring project activities with the team working methodologies defined;
- Articulate the incorporation of the management experience of the management partner of the consortium.

5. Evaluation Strategy

The evaluation strategy to verify the outreach and coverage of the activities and results will be a continuous monitoring, all along the 4 phases, of the main project outcomes to be produced, using the working methodology and work plan defined:

- 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;
- Communication & Dissemination Plan
- Framework Operation Process;
- HISC4ALL application (proof of concept);
- Website.

Cost effectiveness and financial management *(n/a for prefixed Lump Sum Grants)*

Describe the measures adopted to ensure that the proposed results and objectives will be achieved in the most cost-effective way.

Indicate the arrangements adopted for the financial management of the project and, in particular, how the financial resources will be allocated and managed within the consortium.

⚠ *Do NOT compare and justify the costs of each work package, but summarize briefly why your budget is cost effective.*

Measures adopted to ensure that the proposed results and objectives will be achieved in the most cost-effective way

In order to be efficient and make a correct rationalization of resources, it is essential to observe the good practices recommended for co-financed projects, limiting any type of waste, including working hours.

- This implies, first of all, a good planning of all activities, considering an estimated budget.
- The times allocated by the teams to each activity were defined taking into account the rationale underlying the entire project. It must not be forgotten that knowledge production projects, as is the case here, always have a greater degree of difficulty in estimating working times. But for the project to be successful, people from each partner were selected who, taking into account their characteristics, are more apt for the work that is being developed. Your curriculum, experience and internal skills are the guarantee that the activities will go according to plan.
- Strong and pragmatic coordination, always up-to-date and adapting to the problems that arise, will be a sine qua non condition for there to be no deviations from what was planned, either in terms of allocated hours or in terms of costs. Keeping regular meetings, it will be possible to act in a cadenced and preventive way, avoiding possible problems or difficulties from the outset.
- The fact that the Consortium is aware of the market for SMEs and health and healthcare institutions is a guarantee that all the conditions exist to guarantee the database of entities to be used to carry out the various test moments of the construction of the framework.
- Finally, although the staff costs are high, it is necessary not to forget that we are dealing with research work that requires many hours of work, that we are dealing with people with very high skills (some with a PhD degree), but which is fundamental for the credibility and quality of a work and the design of a framework like the one that is intended to be carried out with this project.

Arrangements adopted for the financial management of the project and, in particular, how the financial resources will be allocated and managed within the consortium

Arrangements to be adopted:

- A budget will be created for each of the activities, and for each of the consortium partners, and the way in which resources, including financial ones, will be distributed by each entity will be defined at the outset.
- Monthly, a report will also be made of all costs of each entity, allocating to each activity or budget component, in order to detect any deviations. In coordination meetings, all indicators regarding the progress of activities, costs incurred, and other relevant information will be analysed, with preventive action being taken to rationalize resources, whenever required.
- Since the project costs are defined at the outset for each entity, they will be responsible for their share, up to the ceiling allocated to them. If any of the entities exceeds the defined ceiling, they will be responsible for this increase in costs, and the respective funding will be required, so that in the end there is a balance between the resources used, and the way they were financed by each entity.

2.3 Capacity to carry out the proposed work

Consortium cooperation and division of roles (if applicable)

Describe the participants (Beneficiaries, Affiliated Entities and Associated Partners, if any) and explain how they will work together to implement the project. How will they bring together the necessary expertise? How will they complement each other?

In what way does each of the participants contribute to the project? Show that each has a valid role and adequate resources to fulfil that role.

Note: *When building your consortium you should think of organisations that can help you reach objectives and solve problems.*

Describe the participants – Beneficiaries

The Consortium is composed by three organizations, INEM and Pahldata, all organizations with activity focused in the healthcare sector. The consortium mobilizes a very experienced multidisciplinary team with synergetic and complementary activities. 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 National Institute of Medical Emergency (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 of Medical Emergency, responsible for coordinating the operation of an Integrated System of Medical Emergency that guarantees the very quick 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 of 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 (SIEM). 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.

From the beginning of the current year (2022) until May 2022 INEM already received 528.663 emergency calls which have resulted in 335.786 resource triggering. In 2021 INEM relied on 671 emergency resources to respond to diverse needs.

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

- The activity of the Urgent Patient Guidance Centres (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);
- 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 an organization of the IT sector created in 1987 developing activities for the Banking, Telcos, Manufacturing, Transports, Healthcare and Public sectors, with 48 collaborators. Has participation in Healthcare company that is a Health Sector Information Solutions Provider, with a mission to leverage digital transformation in the healthcare sector. The companies provide value-added solutions to the Portuguese and international health sector that address current and future challenges. Its qualified team is committed to understanding the challenges and problems of customers and therefore seeking to find innovative, disruptive solutions that provide value, materializing in effectiveness and efficiency.

The need to address the trends and demands of the Healthcare sector, when 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.

CHUSJ – 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.

Explain how they will work together to implement the project

Project management will be done in accordance with the PMI methodology. To ensure effective communication, and that decision-making is timely and according to the level of responsibility of each one, there will be three different functional structures described in the responsibility matrix:

Steering Committee		***Responsabilities***
INEM Pahldata CHUSJ	Members of the Board of Directors Project Director	Decision and leadership: - Defines objectives and guidelines - Follows and controls the quality of the project - Makes decision of a strategic scope and/or with financial impact - Defines priorities for action - Unlocks possible barriers to the proper functioning of the project - Analysis and approval of project outputs

Project management		*Responsabilities*
INEM Pahldata CHUSJ	Project Director Project Managers	Guidance, control and management: - Regular reporting and preparation of information for decision making - Conceptual and methodological support - Detailed definition of the activities to be carried out - Quality assurance and/or validation of results - Responsibility for meeting global deadlines - Coordination, guidance and support to operational teams

Project team		*Responsabilities*
INEM Pahldata CHUSJ External consultants	Functional Consultants Technical Consultants	Execution: - Performs the activities provided in the work plan, in accordance with the methodology and quality standards adopted - Prepares project documents and deliverables Functional consultants: - Collaboration in the definition and design of the solution - Support documentation preparation Technical consultants: - Solution architecture design - Integration processes definition

Monitoring the progress of the project will be carried out with periodic meetings:

Meeting	Frequency	Responsibility	Participants
Steering committee	*Monthly*	*Steering committee*	*Steering committee*
Kick-off	*Single meeting*	*Project management*	*Project director* *Project manager* *Consultants* *Stakeholders*
Project management	*Biweekly*	*Project director*	*Project director* *Project manager*
Project follow-up	*Weekly*	*Project manager*	*Project manager* *Functional consultants*
Technical and functional	*Ad-hoc*	*Project manager*	*Project manager* *Project team*

How will they bring together the necessary expertise?

Under the methodology explained above, each element of the consortium will bring its expertise to ensure the success of this project.

INEM and CHUSJ contribute with the know-how and needs from the healthcare providers. Pahldata will bring its expertise as a consulting firm in the health sector with a team with outstanding experience in the information security and cybersecurity.

Both INEM and CHUSJ will contribute with knowledge from the healthcare sector, each one according to its nature and area of activity. INEM will also promote the validations of the HISC4All tool in different Portuguese Public Hospitals for those who drains patients.

How they complement each other

Both INEM and CHUSJ represent different healthcare entities, a hospital and an emergency department, and are custodians of their patients' clinical information. And is concerned about protecting its data from cyberattacks and ensuring information security along the entire data cycle. Moreover, sharing that information with other entities involves trusting the maturity of those entities with respect to information security and cybersecurity, which is not always clear.

Pahldata, as a consulting and technological company focused on healthcare and with a team of experts on information security and cybersecurity, will develop the information security and cybersecurity framework adapted to the needs of healthcare providers.

Both INEM and CHUSJ will contribute with field expertise of healthcare providers so that the framework to be developed will be useful to any healthcare provider.

Way does each of the participants contribute to the project

With Covid-19 pandemic that in a sudden and urgent way shifted the patient care to citizens' homes, healthcare entities got more exposed to cyber-attacks. Therefore, Pahldata saw the need to intensify its Information Security and Cybersecurity offer. It gives to the market a personalized service of monitoring, detection, and response to security incidents, operated by a team of specialists, based on a set of technological solutions, and supported by standards and frameworks to ensure the compliance of the service.

The Consortium networking and security teams proposed to create a new framework to assess the level of maturity of the different actors in the health sector involved in sharing data and information with and within each other. The purpose is to ensure that these exchanges take place between entities that meet certain minimum-security requirements and, to this end, comply with the highest levels of the maturity model to be developed.

To assess the quality and reliability of the framework being developed, as well as to participate with inputs for the project, the project count on INEM and CHUSJ, two prestige healthcare entities with distinct scopes of action.

Project teams and staff

Describe the project teams and how they will work together to implement the project.

List the staff included in the project budget (budget category A) by function/profile (e.g. project manager, senior expert/advisor/researcher, junior expert/advisor/researcher, trainers/teachers, technical personnel, administrative personnel etc. and describe briefly their tasks.

Name and function	Organisation	Role/tasks/professional profile and expertise
Paulo Pinto **Project Manager**	INEM	The Project Manager coordinates the teams, activities, and responsibilities of the respective Consortium Member.
Filipe Botas **Senior Expert / Adviser / Researcher**	INEM	Develop tasks within the scope of the project activities described for the Consortium Team. Interacting with the other Consortium members in the technical activities of the project. Participate in the practical, testing and validation activities of the Project, as stakeholders form the healthcare sector.
José Ferreira **Junior Expert / Adviser / Researcher**	INEM	Develop tasks within the scope of the project activities described for the Consortium Team. Interacting with the other Consortium members in the operational activities of the project. Participate in the practical, testing and validation activities of the Project, as stakeholders form the healthcare sector.
Gustavo Oliveira **Technical Personnel**	INEM	Develop tasks within the scope of the project activities described for the Consortium Team.

		Interacting with the other Consortium members in the technical activities of the project. Participate in the practical, testing and validation activities of the Project, as stakeholders form the healthcare sector.
Paula Moreno **Administrative Personnel**	INEM	Develop tasks within the scope of the project activities described for the Consortium Team. Interacting with the other Consortium members in the administrative activities of the project. Participate in the practical, testing and validation activities of the Project, as stakeholders form the healthcare sector.
Sónia Nascimento **Project Director**	Pahldata	The Project Director will oversee the project managers and ensure the successful conclusion of the project. Will be present at the Steering Committees. This person will have the following responsibilities: • Alignment of the project with the defined objectives • Strategic decision making • Evaluation of the project's evolution
Alberto Caria **Project Manager**	Pahldata	The Project Manager coordinates the teams, activities, and responsibilities of the respective Consortium Member. This person will have the following responsibilities: • Project planning • Project progress control • Responsibility for project follow-up meetings • Scheduling of deliveries • Management and control of changes to the project schedule Assure the execution of the following tasks: • Execution of Questionnaires and Data Processing • Conducting Interviews and Transcription • Project report writing • Support for the design of Outputs • Conducting a Focus Group • Training, Awareness and Training Program
José Martins, **Senior Information Security and Cyber Security Expert**	Pahldata	The Senior Information Security and Cyber Security Expert creates and explores security measures to protect the organization’s information. This person will have the following responsibilities: • Coordination and execution of the design of Outputs • Framework Implementation Process Coordination (Action Research) Assure the execution of the following tasks: • Literature Review and document analysis of the main national and international approaches to Information Security and Cybersecurity • Use cases / UML • Review and validation of project outputs • Support for reporting

		Expertise • Research method and research techniques (Design Science) • Lead implementer 27001 e Lead Manager 27002 • Recommended with at least one of the following certifications: CISM or CISSP • Attack Method Modeling Techniques
Luis Dias / Agostinho Valente / Carlos Alexandre **Senior Information Security and Cyber Security Expert**	Pahldata	The Senior Information Security and Cyber Security Expert creates and explores security measures to protect the organization's information. This person will have the following responsibilities: • Coordination and execution of the design of Outputs • Framework Implementation Process Coordination (Action Research) Assure the execution of the following tasks: • Literature review and document analysis of the main national and international approaches to Information Security and Cybersecurity • Use cases / UML • Review and validation of project outputs • Support for reporting Expertise • Research method and research techniques (Design Science) • Lead implementer 27001 e Lead Manager 27002 • Recommended with at least one of the following certifications: CISM or CISSP • Attack Method Modeling Techniques
António Galindro **Junior Information Security and Cyber Security Expert**	Pahldata	The junior Information Security and Cyber Security Expert supports the execution of the process of creating and exploring security measures to protect the organization's information. This person will have the following responsibilities: • Coordination and execution of the design of Outputs • Framework Implementation Process Coordination (Action Research) Assure the execution of the following tasks: • Literature review and document analysis of the main national and international approaches to Information Security and Cybersecurity • Use cases / UML • Review and validation of project outputs • Support for reporting Expertise • Research method and research techniques (Design Science) • Lead implementer 27001 and Lead Manager 27002 • Recommended with at least one of the following certifications: CISM or CISSP • Attack Method Modeling Techniques

Jorge Custódio **Senior IT Specialist**	Pahldata	The Senior IT Specialist creates and provide for documentation related to system configurations, mapping, processes, and application management. Assure the execution of the following tasks: • Administration of designated platforms (e.g., Moodle, LimeWare) • Program the designated applications (e.g., Django and Python) • Management of Business Process Management – Automation Process (e.g., Bonita BPM) • OO Database Management System (eg MongoDB) • Support for reporting
José Dinis **Junior IT Specialist**	Pahldata	The Junior IT Specialist creates and provide for documentation related to system configurations, mapping, processes, and application management. Assure the execution of the following tasks: • Administration of designated platforms (e.g., Moodle, LimeWare) • Program the designated applications (e.g., Django and Python) • Business Process Management – Automation Process (e.g., BonitaBPM) • OO Database Management System (eg MongoDB) • Support for reporting
TBI **Senior Healthcare Expert**	Pahldata	Senior consultant that will assure the execution of the following tasks: • Execution of Questionnaires and Data Processing • Conducting Interviews and Transcription • Project report writing • Support for the design of Outputs • Conducting a Focus Group • Training, Awareness and Training Program Academic background on Biomedical Engineer or similar with more than five year of experience on healthcare consulting.
TBI **Junior Healthcare Expert I**	Pahldata	Junior consultant that will execute the following tasks: • Conducting Interviews and Transcription • Project report writing • Support for the design of Outputs • Conducting a Focus Group • Training, Awareness and Training Program • Translation of the tool and website into English Academic background on Biomedical Engineer or similar with more than one year of experience on healthcare consulting.
TBI **Junior Healthcare Expert II**	Pahldata	Junior consultant that will execute the following tasks: • Execution of Questionnaires and Data Processing • Conducting Interviews and Transcription • Project report writing • Support for the design of Outputs • Conducting a Focus Group • Training, Awareness and Training Program

		• Translation of the tool and website into English Academic background on Biomedical Engineer or similar with more than one year of experience on healthcare consulting.
Maria João Campos **Project Manager**	CHUSJ	The Project Manager coordinates the teams, activities, and responsibilities of the respective Consortium Member.
Nelson Pereira **Senior Expert / Adviser / Researcher**	CHUSJ	Develop tasks within the scope of the project activities described for the Consortium Team. Interacting with the other Consortium members in the technical activities of the project. Participate in the practical, testing and validation activities of the Project, as stakeholders form the healthcare sector.
Carla Ávila **Junior Expert / Adviser / Researcher**	CHUSJ	Develop tasks within the scope of the project activities described for the Consortium Team. Interacting with the other Consortium members in the operational activities of the project. Participate in the practical, testing and validation activities of the Project, as stakeholders form the healthcare sector.
Cristina Araujo **Technical Personnel**	CHUSJ	Develop tasks within the scope of the project activities described for the Consortium Team. Interacting with the other Consortium members in the technical activities of the project. Participate in the practical, testing and validation activities of the Project, as stakeholders form the healthcare sector.

Outside resources (subcontracting, seconded staff, etc) *If you do not have all skills/resources in-house, describe how you intend to get them (contributions of members, partner organisations, subcontracting, etc.) and for which role/tasks/professional profile/expertise* *If there is subcontracting, please also complete the table in section 4.*
Contributions of Outside Resources – subcontracting. Role/tasks/professional profile/expertise **Mundi Consulting** – www.mundiconsulting.net ***Expertise*** Mundi Consulting is an international consulting company that provides services and develops solutions for strategic and operational management, human resources and training, international procurement and cooperation for development. Since 1988, Mundi Consulting operates in Portugal, Cape Verde, Mozambique, Sao Tome and Principe, Guinea-Bissau, Angola East-Timor and Brazil, on an ongoing basis, both with own resources or in partnerships with local companies and experts. Mundi Consulting delivers management solution services to companies, business groups, business associations, chambers of commerce, central, regional and local government, other public institutions and governmental organizations, non-governmental organizations, financial institutions, bilateral and multilateral agencies and organizations, economic and business development promoters. Expertise of Mundi Consulting within the scope of this Project.

- 34 years of experience in project design and submission of applications for incentive systems to finance projects;
- 25 years of experience in the International Development Cooperation market;
- 25 years of experience in carrying out economic, social, institutional and business capacity building and development projects, with funding from Institutions and international development support funds, through a direct approach to donors or integrated in application windows and incentive systems.

Role

Assisting & Monitoring the application of project activities into the Stakeholders, including:

- Assist the structuring the Database of the different stakeholders and its involvement in the project: 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).
- Support the Application of questionnaires and interviews to these stakeholders
- Supervise the data collection and information treatment;
- Guarantee the quality control on the preparation of Design phase's reports
- Support the implementation of methodological approach in the development of the Focus Groups / Use Cases.
- Assist the conception the capacity & training activities that should be developed to consolidate the implementation of the Framework;
- Guarantee the quality control of the phases 2, 3 and 4 reports.

Another organization

To support the activities to be developed by the Consortium within the implementation of the HISC4ALL project, it will also participate the following Organization:

PALCONSULTING – www.palconsulting.pt

Expertise

PALCONSULTING is a management consulting firm, established to leverage technical and business knowledge in an era where "Management & Data" go "hand in hand" and organizational, digital transformation are a must-be. PALCONSULTING works with Governments, Multilaterals and Private Developers, in shaping public policy, reforms and structuring bankable projects. PALCONSULTING assistance spans across various sectors including Agriculture & Poultry, Tourism & Leisure, Transport, Health, Public Sector, Industry and Corporate.

PALCONSULTING business focus is structured to respond to current market concerns and trends through:

Problem solving and minimizing risk
Supporting management decisions
Streamline, enhance and automate processes
Reinforcing security
Ensuring operational and business continuity
Empowering teams
Providing support in research and funding applications

PALCONSULTING main capabilities are:

- Intelligence in Business and Operations;
- Data Analysis and Technological Tools;
- Information Security, **Cybersecurity,** GDPR and Risk;
- Value Management Office.

PALCONSULTING has national and international experience in the conceptualization, surveying, and implementation of corporate architectures solutions, namely in the organizational, procedural, information systems and risk management aspects.

Main Certifications:

6σ
PMI
DA SENIOR SCRUM MASTER
CSM
CERTIFIED
A-CSM
CERTIFIED
SA
SAFe 5
ISO
27001
PECB
ISO/IEC 27001
PECB
ISO/IEC 27002
CRISC
C|CISO
TRAINED
SA
SAFe 6
PMI
PMP
PMI
PMI-ACP
CCP
UiPath
Robotic Process Automation
UiPath Partner

Roles

Support Technical Knowledge Information Security and Cybersecurity

Incorporate in the framework several activities with knowledge and strong experience of organizations with expertise over 30 years in the area of information security and cybersecurity in the health sector, including knowledge:

- In activities of preparing and implementing certifications in ISO standards (27001/31000, other) and Portuguese Standards of Cybersecurity;
- In activities of "Assessment" for business processes and technical platforms/infrastructures.
- In activities of business and technical Proof-of-Concepts.

Assisting Project Development & Support the execution of Market Tests

Support the management process of implementing the wide market testing all along the project, near the wide group of 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), including:

- Playing the leading role in "Assessment" activities, both in terms of ISO 27001 controls and those related to the information flows supporting the Use Cases.
- Support and contribute for validation contents of the framework conception and update versions.
- Support the conception of the website;
- Support the structuring and development of the Communication & Implementation Plans.
- Support in activities of global framework validation, namely conduct and follow the "Proof-of-Concept" – POC method.
- Support in activities related with documentation and media artifacts.

Consortium management and decision-making risk(if applicable)

Explain the management structures and decision-making mechanisms within the consortium. Describe how decisions will be taken and how regular and effective communication will be ensured. Describe methods to ensure planning and control.

Note: *The concept (including organisational structure and decision-making mechanisms) must be adapted to the complexity and scale of the project.*

The Consortium created between INEM, Pahldata and CHUSJ 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 Member will grant the Consortium Leader the powers that, in each case, are necessary for the exercise of their functions, by means of an appropriate legal instrument.

Consortium Member 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) Inform about the progress of the works;

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

Consortium Member is 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 it makes during the execution of the work and undertakes to recover them by itself or at its own expense.

3. IMPACT

3.1 Expected outcomes and deliverables — Dissemination and communication

Expected outcomes and deliverables

Define and explain the extent to which the project will achieve the expected impacts listed in Call document.

Presentation of Outcomes and Deliverables - Extent to which the project will achieve the expected impacts listed in Call document

Information security and cybersecurity in the healthcare sector are of utmost importance. Not only because of the sensitivity of clinical information but also because of the advantages of data sharing between systems of the same entity and between entities. In addition, more and more cases of cyber-attacks are being hold on healthcare providers.

The present project aims to address this fragility and will culminate in the creation of a self-assessment and best practices prescribing tool (HISC4All) to be used by all entities that process and share clinical information. All these entities will be able to perform the self-assessment online and receive an automated report on the controls to improve its information security and cybersecurity.

The development of HISC4All framework is based on a set of concepts already defined in reference academic disciplines related to Information Security, Information Systems and Cybersecurity and/or in national or international standards and focusing them for health date and healthcare providers and its validation on the use cases defined. Furthermore, with its materialization in a self-assessment tool to be made available to all entities in scope addresses the four main impacts of the Call:

1. Implementation of objectives and requirements under the NIS Directive in relation to the health sector;
2. Adoption in healthcare and health institutions, and in particular SMEs, of tools, methods, organisational and management practices dedicated to cybersecurity. Also, the exchange of information between peers;
3. Cybersecurity education, awareness and skills development in healthcare and health institutions.

The success of the implementation of a framework like this one depends greatly on a training and awareness program for the Organization's employees. Therefore, following the design of the Framework and the associated implementation and operation processes, a general five-phase training, awareness and education program will be designed with the main objective of ensuring the efficient and effective implementation and operation of the Framework and reinforce the impact expected on "Cybersecurity education, awareness and skills development in healthcare and health institutions".

Finally, as an ultimate achievement by using HISC4All self-assessment tool, all healthcare entities, particularly those with less experience in information security and cybersecurity, gain a greater understanding of their HISC4All maturity level and become aware of the path to take to improve it. Also, healthcare entities will be more likely to share information with others that are well classified on HISC4All and thus improving the care provided to their patients, according to the benefits of interoperability in healthcare.

Dissemination and communication of the project and its results

If relevant, describe the communication and dissemination activities, activities (target groups, main messages, tools, and channels) which are planned in order to promote the activities/results and maximise the impact. The aim is to inform and reach out to society and show the activities performed, and the use and the benefits the project will have for citizens

Clarify how you will reach the target groups, relevant stakeholders, policymakers and the general public and explain the choice of the dissemination channels.

Describe how the visibility of EU funding will be ensured.

⚠ *In case your proposal is selected for funding, you will have to provide a more detailed plan for these activities (dissemination and communication plan), within 6 months after grant signature. This plan will have to be periodically updated; in line with the project progress.*

Dissemination and communication activities are fundamental for the success of this project.

The communication strategy and the respective activities, planned within the scope of the project, will contribute to disseminate the results obtained and promote the use of the HISC4All (self-assessment tool developed) so that healthcare entities are more aware of areas regarding information security and cybersecurity.

Communication and dissemination activities, activities (target groups, main messages, tools, and channels) planned in order to promote the activities/results and maximise the impact

During the development of the communication plan the following target stakeholders where identified:

- Hospital and Clinics;

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

The set of the activities described below guarantees that all the stakeholders increase their sensibility and self-awareness of information security and cybersecurity and how can they improve it.

The communication plan includes the creation of a website where all relevant information about the project will be shared, such as its scope, goals and lessons learned. Here it will also be made available the self-assessment tool. Additionally, all promoters will share this information on their institutional websites, LinkedIn and other direct communication channels that they currently use.

This plan also includes Workshops and Webinars and the activities of preparing its contents.

Finally, for a major cross border dissemination that also includes the academia, to set this framework as a reference, a scientific paper will be presented at a conference.

For dissemination purposes, all communication related to this framework project will be available in Portuguese and English.

Clarify how to reach the target groups, relevant stakeholders, policymakers and the general public. Explain the choice of the dissemination channels.

First, by making the communication materials available in English, any healthcare entity from the European Union will be able to access the project information and the self-assessment tool made available with the website.

Via LinkedIn we will reach entities with whom none of the consortium members have direct relationship. Also, by email, or other mean of communication of the consortium members, specific entities previously defined to be of interest for this project will be contacted.

How the visibility of EU funding will be ensured.

All the communication and dissemination of the framework will follow the requirements of an EU funding program including the logos. The website created for purposes of external communication of the framework intends also to promote the EU funding.

During the workshops and webinars mentioned above, it will be promoted the visibility of EU funding throughout the events as well as in all the documents produced for this purpose.

3.2 Competitiveness and benefits for society

Competitiveness and benefits for the society

Describe the extent to which the project will strengthen competitiveness and bring important benefits for society

Extent to which the project will strengthen competitiveness and bring important benefits for society

Cyberattacks have extreme impacts on healthcare, not only to the entities but also to professionals and patients:

- It compromises data, which in healthcare is highly sensitive;
- It disrupts the delivery of care which can ultimately lead to the cancellation of all hospital activity.

In the past few years there was an increase in the number of cyber-attacks around the world and, during the Covid-19, Healthcare was the most targeted industry. According to a study from Check Point® Software Technologies Ltd., at a global level, in the fourth quarter of 2020, there was a 45% increase in the number of cyberattacks, mainly ransomware, on hospitals worldwide and mostly in Central Europe. A study from CyberPeace Institute, from January to February 2022, reports a geographical shift on the targeted organizations, with a 22% increase in Europe and 22% decrease in the United States of America.

The susceptibility to cyberattacks in this sector also grows with automation, interoperability and data analytics. Therefore, to be able to take advantage of the latest technological advances with quality and confidence, healthcare organizations must ensure compliance with information security and cybersecurity requirements.

Nevertheless, not all healthcare entities have the resources to invest in information security and cybersecurity, nor are aware that they can also be targeted. This is the reason why this framework, being of great importance to hospital, is also of utmost importance to healthcare SMEs like small hospitals, clinical, dentist, pharmacies.

The adoption of frameworks that protect entities from cyberattacks and their data throughout the value chain is vital for these entities that should focus on their mission to deliver quality healthcare.

4. WORK PLAN, TIMING AND SUBCONTRACTING

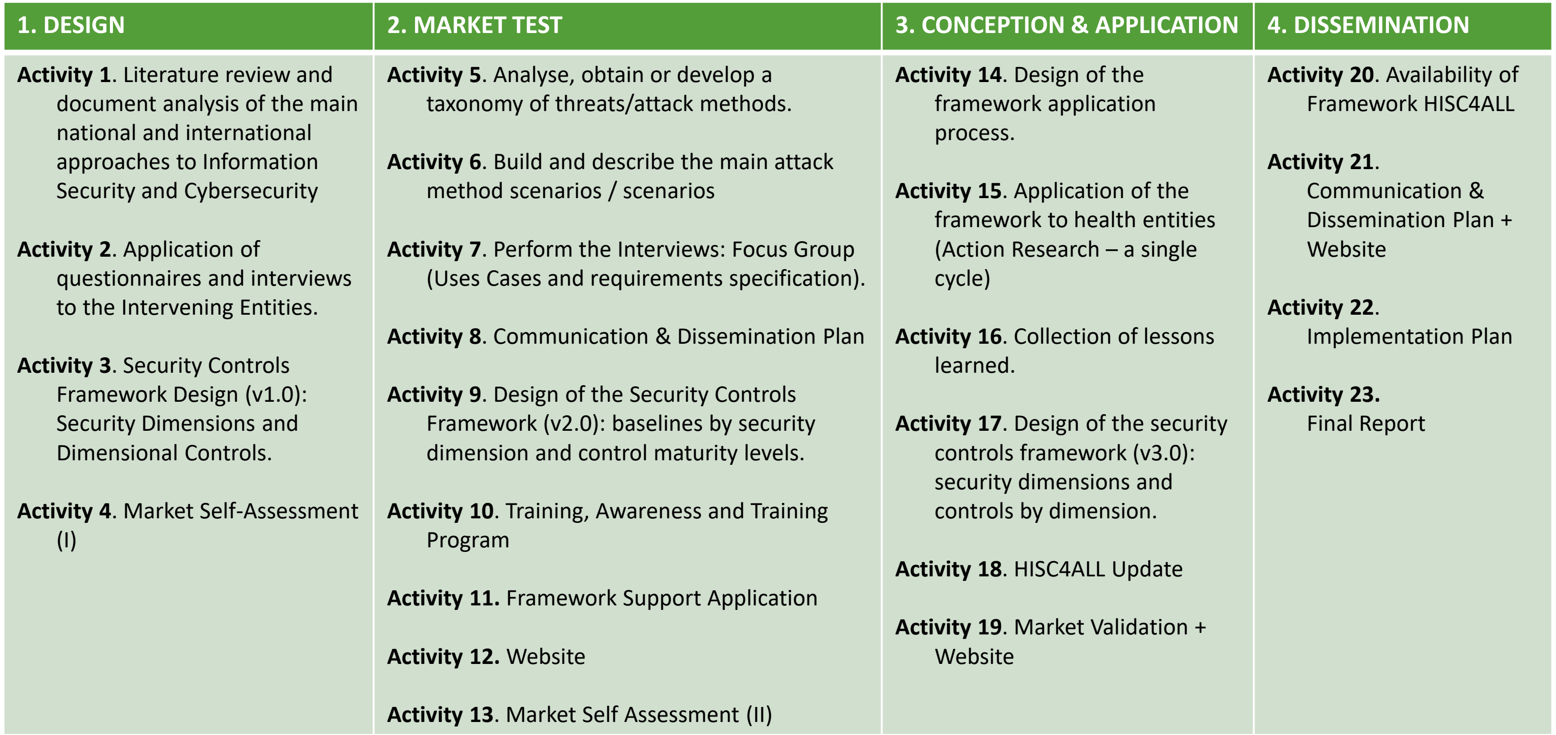
4.1 Work plan

Work plan

Provide a brief description of the overall structure of the work plan (list of work packages or graphical presentation (Pert chart or similar)).

Brief description of the overall structure of the work plan (list of work packages or graphical presentation.

Activities to be developed in the project in each of the Phase:



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**. Communication & Dissemination Plan **Activity 9**. Design of the Security Controls Framework (v2.0): baselines by security dimension and control maturity levels. **Activity 10**. Training, Awareness and Training Program **Activity 11.** Framework Support Application **Activity 12.** Website **Activity 13**. Market Self Assessment (II)	**Activity 14**. Design of the framework application process. **Activity 15**. Application of the framework to health entities (Action Research – a single cycle) **Activity 16**. Collection of lessons learned. **Activity 17**. Design of the security controls framework (v3.0): security dimensions and controls by dimension. **Activity 18**. HISC4ALL Update **Activity 19**. Market Validation + Website	**Activity 20**. Availability of Framework HISC4ALL **Activity 21**. Communication & Dissemination Plan + Website **Activity 22**. Implementation Plan **Activity 23.** Final Report

Figure 13 – Project Phases and Activities

Working Plan & Organization of the Activities

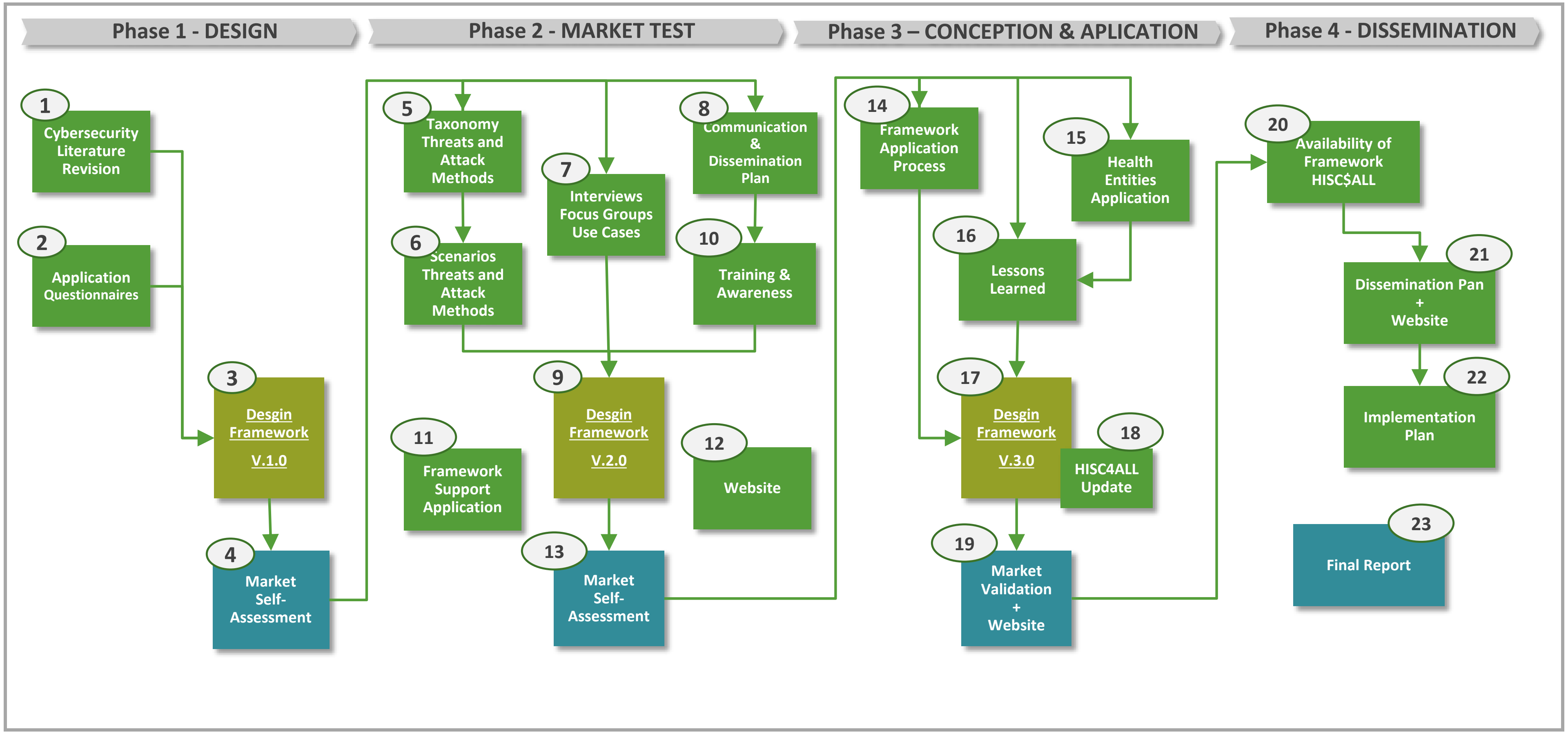
As presented before, and here remembered, the overall structure of the work plan, with the list of the phases and activities, corresponding to the work packages, and a graphical presentation of the organization of the activities, including the sequence of development of each activity and the connections between them.

Project General Working Plan

Phases (1º Year)	Main Activities	Resources	Risks	Indicators
I **(4 months)** (Month I a IV)	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. 2. Application of questionnaires and interviews to the Intervening Entities. 3. Security Controls Framework Design (v1.0): Security Dimensions and Dimensional Controls. 4. Market Self-Assessment (I)	- National / international standards and references. - Elements for application of questionnaires and interviews.	- Delay in applying questionnaires and conducting interviews (Low Risk).	*SegInfo and Cyber controls framework ** (v1.0). Partial report of project no. 1. (Output: Framework v1.0)
II **(8 months)** (Month V a XII)	5. Analyze, obtain or develop a taxonomy of threats/attack methods. 6. Build and describe the main attack method scenarios / scenarios (use attack method modelling techniques and Use Cases). 7. Perform the Interviews: Focus Group (Uses Cases and requirements specification). 8. Design of the Security Controls Framework (v2.0): baselines by security dimension and control maturity levels. 9. Training, Awareness and Training Program in the implementation and operation of the Framework (v1.0). 10. Framework Support Application 11. Website 12. Market Self-Assessment (II)	- Taxonomy of attack methods (main scenarios). - Elements for the realization of the Focus Group. - Software for modeling attack methods and building Use Cases / Requirements (eg astah professional - Open Source Software: LMS Moodle	- Lack of taxonomy (Low Risk). - Failures in carrying out the Focus Group (Low Risk). - Obtaining and competences in the use of applications: astah professional, Moodle (Low or Almost Zero Risk).	Specification of Requirements based on Use Cases. Security Controls Framework (v2.0). Partial report of project no. 2. (Output: Framework v2.0 and Training, Awareness and Training Program in the implementation and operation of the Framework (v1.0).

Project General Working Plan (cont.)

Phases (2º Year)	Main Activities	Resources	Risks	Indicators
III **(10 months)** (Month I a X)	13. Design of the framework application process. 14. Application of the framework to health entities (Action Research – a single cycle) 15. Collection of lessons learned. 16. Design of the security controls framework (v3.0): security dimensions and controls by dimension. 17. HISC4ALL update 18. Market Validation + Website	- International standards. - Entities / Organizations to apply the framework *(proof of concept: one baseline per dimension of the framework)*	- Availability of Entities /Organizations to apply the framework (Low Risk).	*Framework Application Process (v1.0).* *Security Controls Framework (v3.0).* *Partial report of project no. 3.* *(Outputs: Framework v3.0 and Application Process)*
IV **(2 months)** (Month XI e XII)	19. Availability of the HISC4All Tool 20. Communication & Dissemination Plan + Website 21. Implementation Plan 22. Final Report	-	-	*SegInfo Framework and Cybersecurity.* *Final Framework* *Application Process* Implementation Plan Communication & Dissemination Plan Final Project Report. (Outputs: Framework v3.0, Application Process, Operation Process and Final Training, Awareness and Training Program for the implementation and Operation of the Framework).


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
Communication & Dissemination Plan
9
Desgin Framework V.2.0
10
Training & Awareness
11
Framework Support Application
12
Website
13
Market Self-Assessment
14
Framework Application Process
15
Health Entities Application
16
Lessons Learned
17
Desgin Framework V.3.0
18
HISC4ALL Update
19
Market Validation + Website
20
Availability of Framework HISC$ALL
21
Dissemination Pan + Website
22
Implementation Plan
23
Final Report

4.2 Timetable

Timetable (projects up to 2 years)

Fill in cells in beige to show the duration of activities. Repeat lines/columns as necessary.

Note: *Use the project month numbers instead of calendar months. Month 1 marks always the start of the project. In the timeline you should indicate the timing of each activity per WP.*

ACTIVITY	MONTHS																							
	M 1	M 2	M 3	M 4	M 5	M 6	M 7	M 8	M 9	M 10	M 11	M 12	M 13	M 14	M 15	M 16	M 17	M 18	M 19	M 20	M 21	M 22	M 23	M 24
Task 1 - Literature Rev.	■																							
Task 2- Appl. Question.		■	■																					
Task 3 - Framework 1.0			■	■																				
Task 4 - Market Test				■																				
Task 5 - Taxon. Attacks					■																			
Task 6 - Scenarios Attac.					■																			
Task 7 - Interv + Focus G						■																		
Task 8 – Comm.&Dissem						■	■																	
Task 9 - Framework 2.0 .							■	■	■	■														
Task 10 - Training Aware										■														
Task 11 - Fram Support										■	■													
Task 12 - Website												■												
Task 13 - Market Test													■											

Task 14 - Fram Applic														■										
Task 15 - Health Applic														■	■									
Task 16 - Lessons Lern.															■	■								
Task 17 - Framework 3.0																■	■	■	■	■				
Task 18 - UISC4ALL upd																					■	■		
Task 19 - Market + Webs																						■		
Task 20 - Availab Fram.																							■	
Task 21 - Comm+ Webs																							■	
Task 22 - Implem Plan																								■
Task 23 – Final Report																								■

4.3 Subcontracting

Subcontracting

Give details on subcontracted project tasks (if any) and explain the reasons why (as opposed to direct implementation by the Beneficiaries/Affiliated Entities).

Subcontracting — Subcontracting means the implementation of 'action tasks', i.e. specific tasks which are part of the EU grant and are described in Annex 1 of the Grant Agreement.

***Note:** Subcontracting concerns the outsourcing of a part of the project to a party outside the consortium. It is not simply about purchasing goods or services. We normally expect that the participants have sufficient operational capacity to implement the project activities themselves. Subcontracting should therefore be exceptional.*

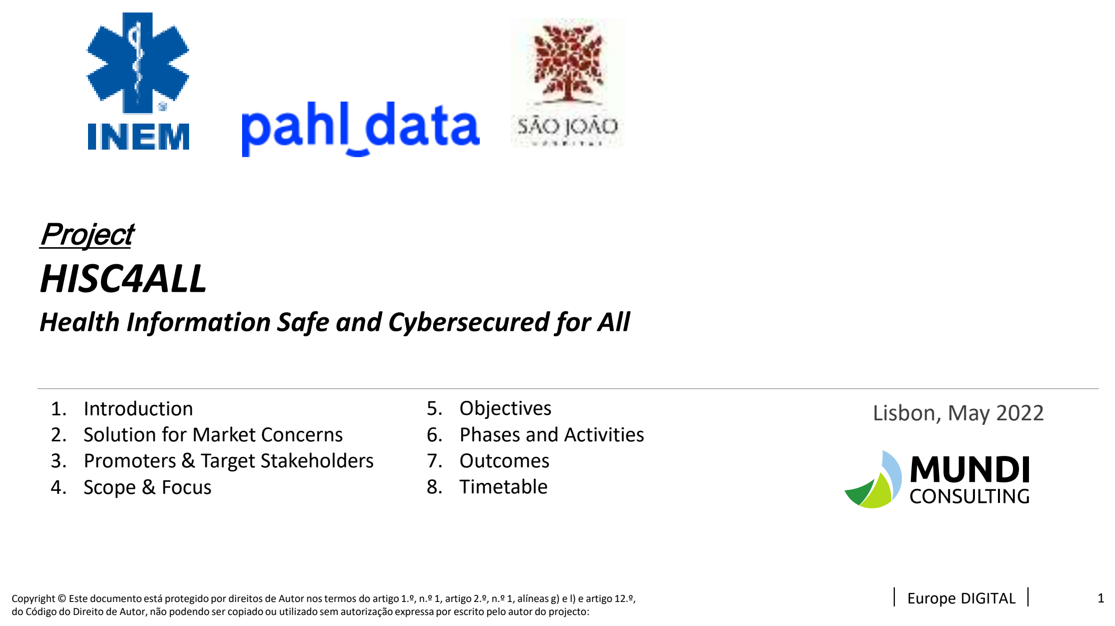
Include only subcontracts that comply with the rules (i.e. best value for money and no conflict of interest; no subcontracting of coordinator tasks).

Work Package No	Subcontract No (continuous numbering linked to WP)	Subcontract Name (subcontracted action tasks)	Description (including task number and BEN to which it is linked)	Estimated Costs (EUR)	Justification (Why is subcontracting necessary?)	Best-Value-for-Money (How do you intend to ensure it?)
1	1	Assisting & Monitoring the application of project activities into the Stakeholders	1	34.624,50 EUR	External entity with more than 30 years of experience in the preparation of international projects and applications	Continuous and permanent monitoring of compliance with the Specifications
2 and 3	2	Support Technical Knowledge Information Security and Cybersecurity	5 to 12 and 13 to 18	61.500 EUR (50% per WP)	Entity with more than 20 years of experience in information security, management and cybersecurity	Continuous and permanent monitoring of compliance with the Specifications
3	3	Assisting Project Development & Support the execution of Market Tests	13 to 18	51.045 EUR	Entity to support the carrying out of Market tests and development of Project activities	Continuous and permanent monitoring of compliance with the Specifications

Other issues: *If subcontracting for the entire project goes beyond 30% of the total eligible costs, give specific reasons.*	There are no Activities subcontracted. The indicated subcontracted entities will develop specific activities all along the project implementation.

5. ANNEXES

5.1 Project Outline



Project

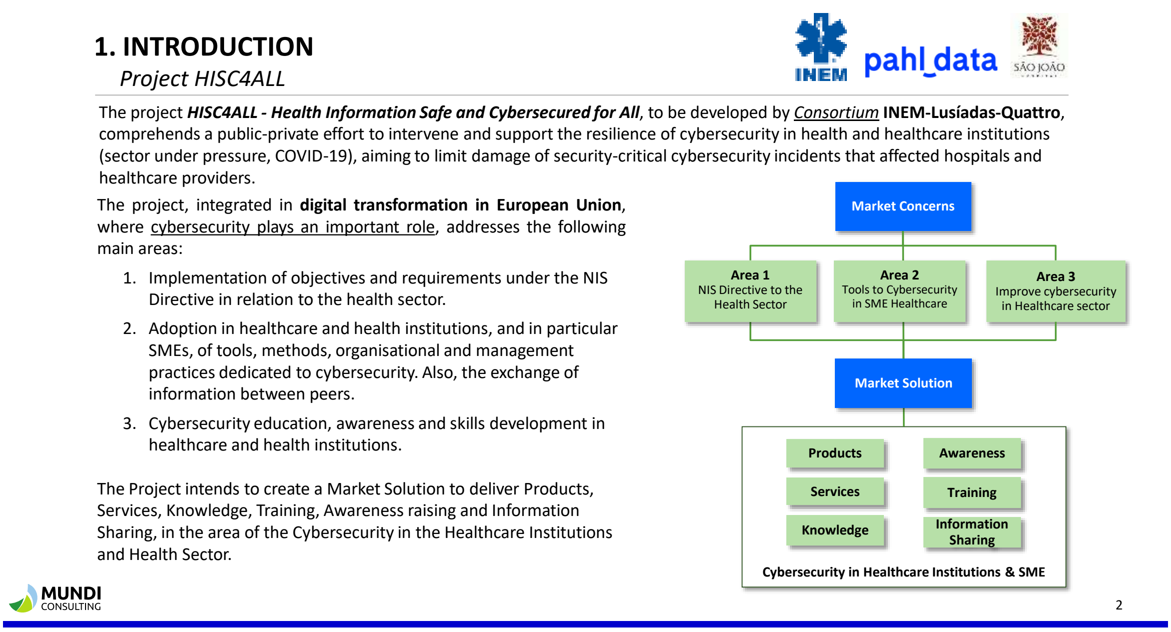
HISC4ALL

Health Information Safe and Cybersecured for All

1. Introduction
2. Solution for Market Concerns
3. Promoters & Target Stakeholders
4. Scope & Focus
5. Objectives
6. Phases and Activities
7. Outcomes
8. Timetable

Lisbon, May 2022

Europe DIGITAL 1



1. INTRODUCTION

Project HISC4ALL

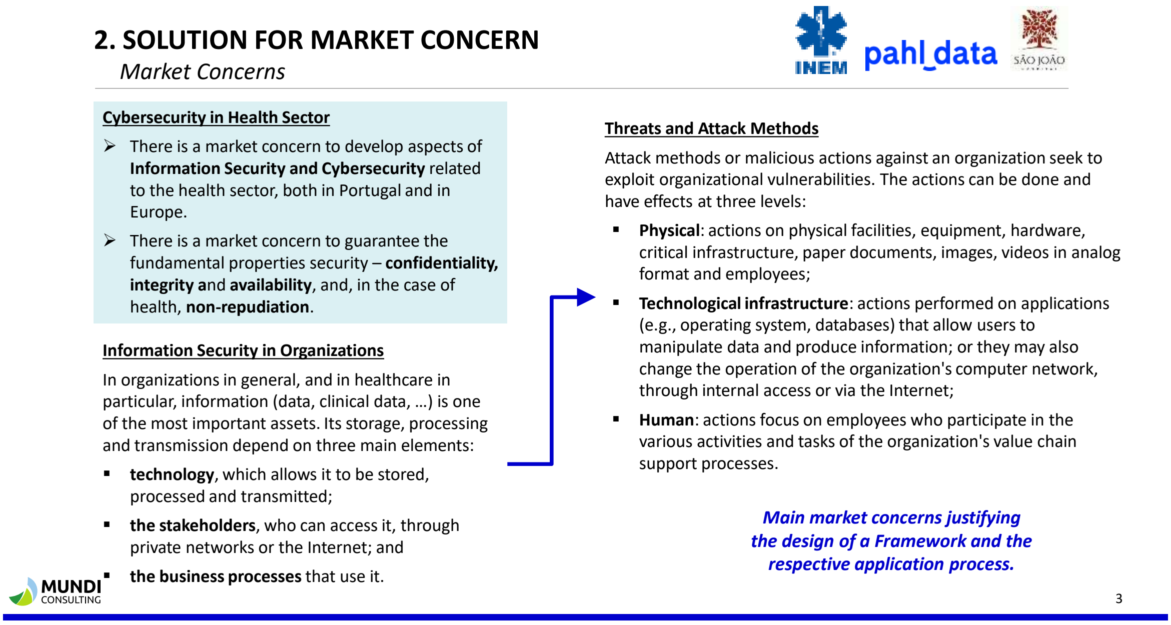
The project ***HISC4ALL - Health Information Safe and Cybersecured for All***, to be developed by *Consortium* **INEM-Lusíadas-Quattro**, comprehends a public-private effort to intervene and support the resilience of cybersecurity in health and healthcare institutions (sector under pressure, COVID-19), aiming to limit damage of security-critical cybersecurity incidents that affected hospitals and healthcare providers.

The project, integrated in **digital transformation in European Union**, where cybersecurity plays an important role, addresses the following main areas:

1. Implementation of objectives and requirements under the NIS Directive in relation to the health sector.
2. Adoption in healthcare and health institutions, and in particular SMEs, of tools, methods, organisational and management practices dedicated to cybersecurity. Also, the exchange of information between peers.
3. Cybersecurity education, awareness and skills development in healthcare and health institutions.

The Project intends to create a Market Solution to deliver Products, Services, Knowledge, Training, Awareness raising and Information Sharing, in the area of the Cybersecurity in the Healthcare Institutions and Health Sector.

Market Concerns
Area 1
NIS Directive to the Health Sector
Area 2
Tools to Cybersecurity in SME Healthcare
Area 3
Improve cybersecurity in Healthcare sector
Market Solution
Products
Awareness
Services
Training
Knowledge
Information Sharing
Cybersecurity in Healthcare Institutions & SME
INEM
pahl data
SÃO JOÃO
MUNDI CONSULTING
2



2. SOLUTION FOR MARKET CONCERN

Market Concerns

Cybersecurity in Health Sector

- There is a market concern to develop aspects of **Information Security and Cybersecurity** related to the health sector, both in Portugal and in Europe.
- There is a market concern to guarantee the fundamental properties security – **confidentiality, integrity** and **availability**, and, in the case of health, **non-repudiation**.

Information Security in Organizations

In organizations in general, and in healthcare in particular, information (data, clinical data, ...) is one of the most important assets. Its storage, processing and transmission depend on three main elements:

- **technology**, which allows it to be stored, processed and transmitted;
- **the stakeholders**, who can access it, through private networks or the Internet; and
- **the business processes** that use it.

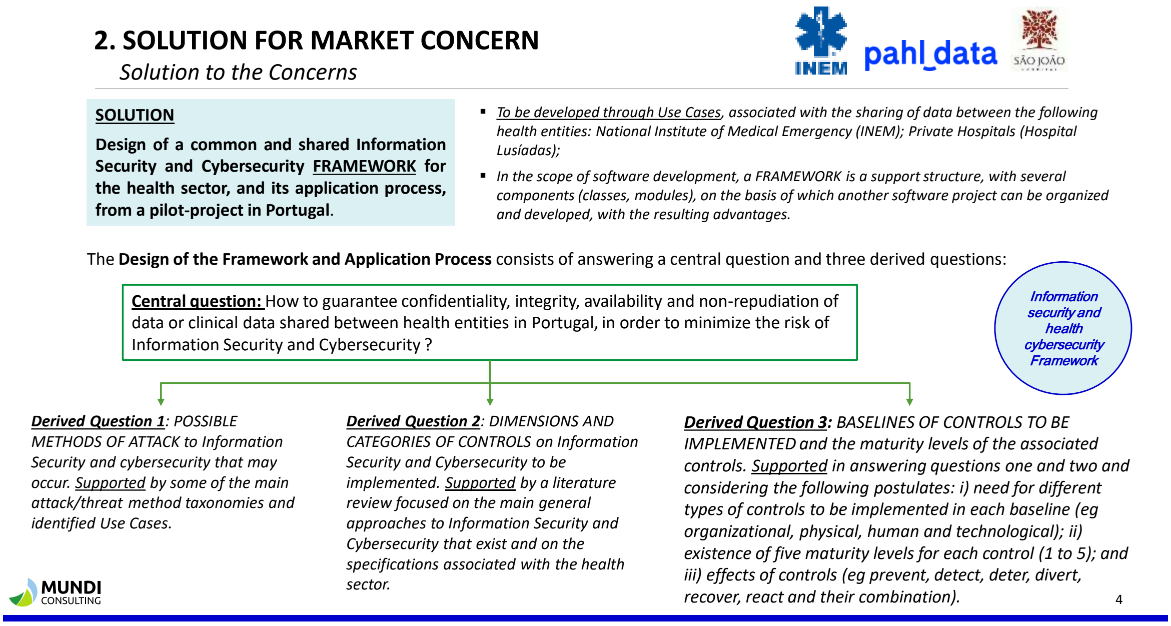
Threats and Attack Methods

Attack methods or malicious actions against an organization seek to exploit organizational vulnerabilities. The actions can be done and have effects at three levels:

- **Physical**: actions on physical facilities, equipment, hardware, critical infrastructure, paper documents, images, videos in analog format and employees;
- **Technological infrastructure**: actions performed on applications (e.g., operating system, databases) that allow users to manipulate data and produce information; or they may also change the operation of the organization's computer network, through internal access or via the Internet;
- **Human**: actions focus on employees who participate in the various activities and tasks of the organization's value chain support processes.

Main market concerns justifying the design of a Framework and the respective application process.

3



2. SOLUTION FOR MARKET CONCERN

Solution to the Concerns

SOLUTION

Design of a common and shared Information Security and Cybersecurity FRAMEWORK for the health sector, and its application process, from a pilot-project in Portugal.

- *To be developed through Use Cases, associated with the sharing of data between the following health entities: National Institute of Medical Emergency (INEM); Private Hospitals (Hospital Lusíadas);*
- *In the scope of software development, a FRAMEWORK is a support structure, with several components (classes, modules), on the basis of which another software project can be organized and developed, with the resulting advantages.*

The **Design of the Framework and Application Process** consists of answering a central question and three derived questions:

Information security and health cybersecurity Framework

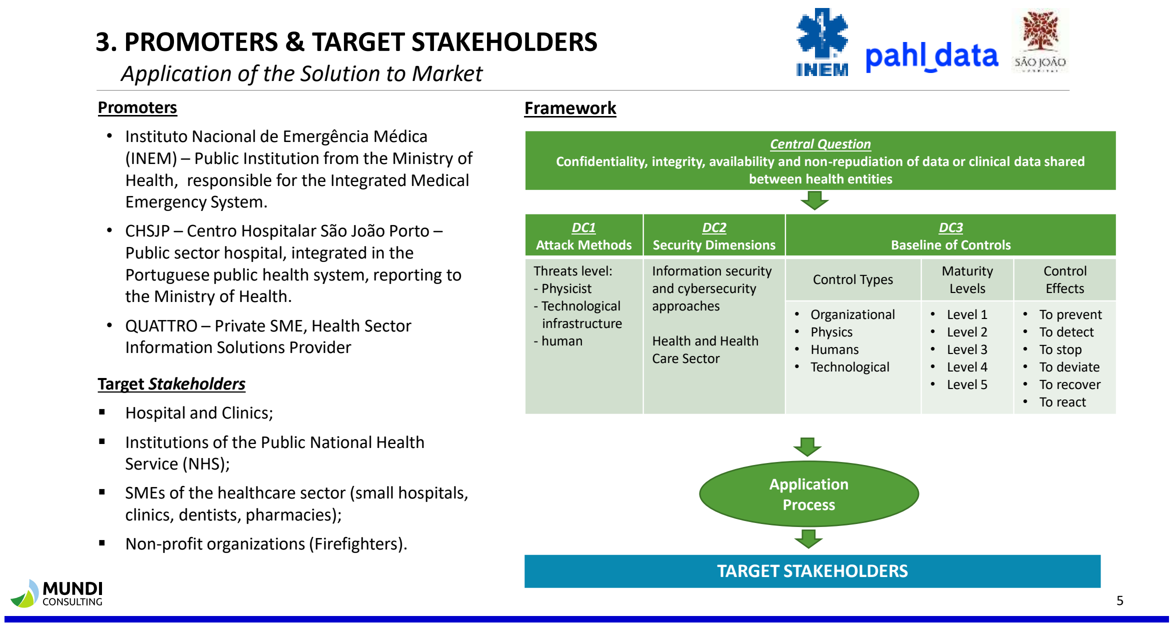
Central question: How to guarantee confidentiality, integrity, availability and non-repudiation of data or clinical data shared between health entities in Portugal, in order to minimize the risk of Information Security and Cybersecurity ?

Derived Question 1: *POSSIBLE METHODS OF ATTACK to Information Security and cybersecurity that may occur. Supported by some of the main attack/threat method taxonomies and identified Use Cases.*

Derived Question 2: *DIMENSIONS AND CATEGORIES OF CONTROLS on Information Security and Cybersecurity to be implemented. Supported by a literature review focused on the main general approaches to Information Security and Cybersecurity that exist and on the specifications associated with the health sector.*

Derived Question 3: *BASELINES OF CONTROLS TO BE IMPLEMENTED and the maturity levels of the associated controls. Supported in answering questions one and two and considering the following postulates: i) need for different types of controls to be implemented in each baseline (eg organizational, physical, human and technological); ii) existence of five maturity levels for each control (1 to 5); and iii) effects of controls (eg prevent, detect, deter, divert, recover, react and their combination).*

4



3. PROMOTERS & TARGET STAKEHOLDERS

Application of the Solution to Market

INEM pahl_data SÃO JOÃO

Promoters

- Instituto Nacional de Emergência Médica (INEM) – Public Institution from the Ministry of Health, responsible for the Integrated Medical Emergency System.
- CHSJP – Centro Hospitalar São João Porto – Public sector hospital, integrated in the Portuguese public health system, reporting to the Ministry of Health.
- QUATTRO – Private SME, Health Sector Information Solutions Provider

Target Stakeholders

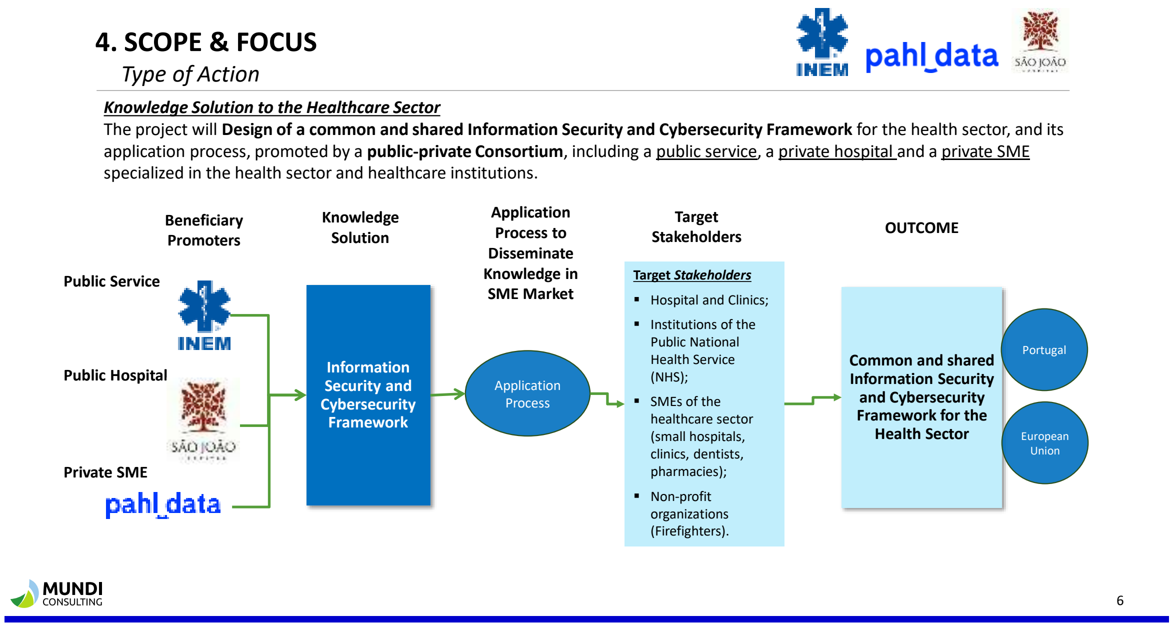
- Hospital and Clinics;
- Institutions of the Public National Health Service (NHS);
- SMEs of the healthcare sector (small hospitals, clinics, dentists, pharmacies);
- Non-profit organizations (Firefighters).

Framework

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**		
Threats level: - Physicist - Technological infrastructure - human	Information security and cybersecurity approaches Health and Health Care Sector	Control Types	Maturity Levels	Control Effects
		• 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

MUNDI CONSULTING 5



4. SCOPE & FOCUS

Type of Action

INEM pahl_data SÃO JOÃO

Knowledge Solution to the Healthcare Sector

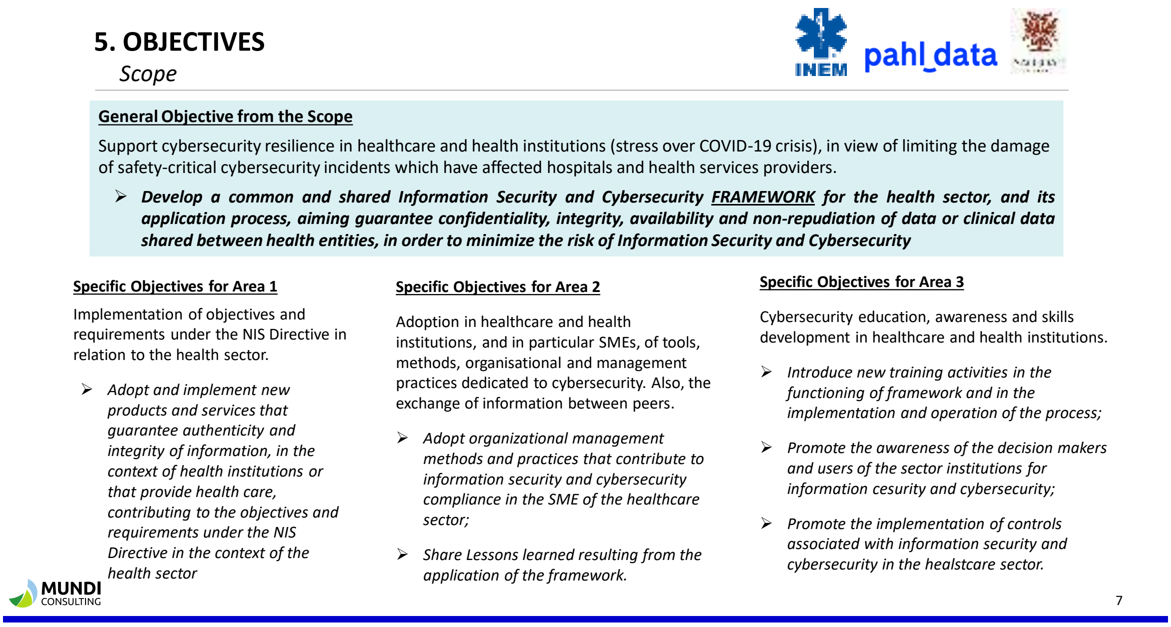
The project will **Design of a common and shared Information Security and Cybersecurity Framework** for the health sector, and its application process, promoted by a **public-private Consortium**, including a public service, a private hospital and a private SME specialized in the health sector and healthcare institutions.

Beneficiary Promoters
Knowledge Solution
Application Process to Disseminate Knowledge in SME Market
Target Stakeholders
OUTCOME
Public Service
INEM
Public Hospital
SÃO JOÃO
Private SME
pahl_data
Information Security and Cybersecurity Framework
Application Process
Common and shared Information Security and Cybersecurity Framework for the Health Sector
Portugal
European Union

Target 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).

MUNDI CONSULTING 6



5. OBJECTIVES

Scope

General Objective from the Scope

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 for Area 1

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*

Specific Objectives for Area 2

Adoption in healthcare and health institutions, and in particular SMEs, of tools, methods, organisational and management practices dedicated to cybersecurity. Also, the exchange of information between peers.

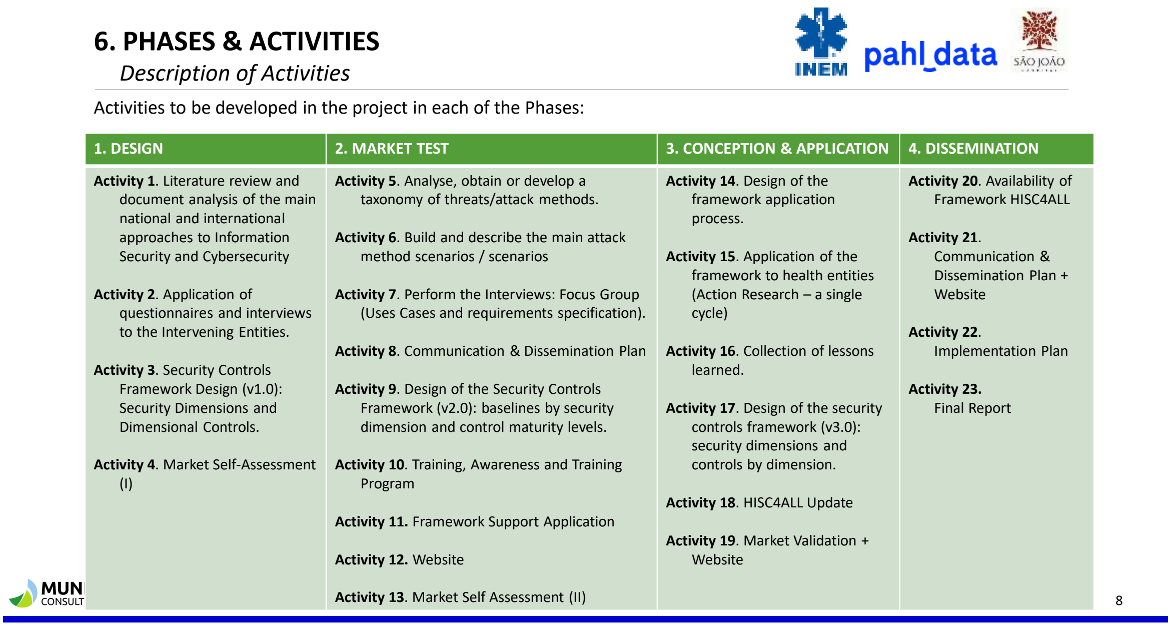
- *Adopt organizational management methods and practices that contribute to information security and cybersecurity compliance in the SME of the healthcare sector;*
- *Share Lessons learned resulting from the application of the framework.*

Specific Objectives for Area 3

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 cesurity and cybersecurity;*
- *Promote the implementation of controls associated with information security and cybersecurity in the healstcare sector.*

7



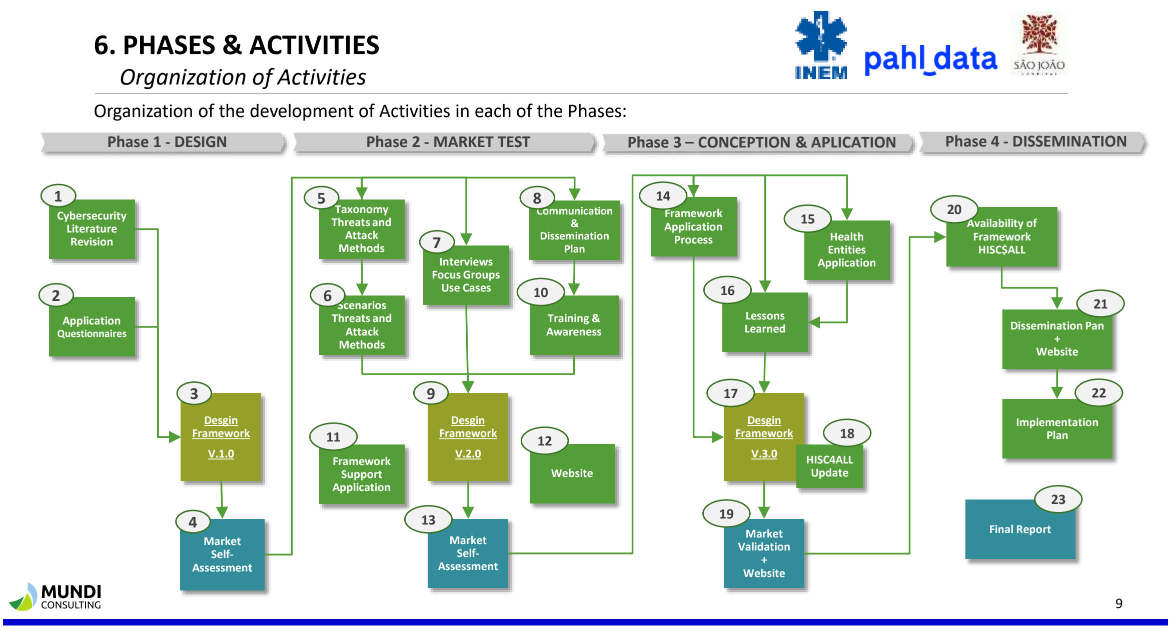
6. PHASES & ACTIVITIES

Description of Activities

Activities to be developed in the project in each of the Phases:

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**. Communication & Dissemination Plan **Activity 9**. Design of the Security Controls Framework (v2.0): baselines by security dimension and control maturity levels. **Activity 10**. Training, Awareness and Training Program **Activity 11.** Framework Support Application **Activity 12.** Website **Activity 13**. Market Self Assessment (II)	**Activity 14**. Design of the framework application process. **Activity 15**. Application of the framework to health entities (Action Research – a single cycle) **Activity 16**. Collection of lessons learned. **Activity 17**. Design of the security controls framework (v3.0): security dimensions and controls by dimension. **Activity 18**. HISC4ALL Update **Activity 19**. Market Validation + Website	**Activity 20**. Availability of Framework HISC4ALL **Activity 21**. Communication & Dissemination Plan + Website **Activity 22**. Implementation Plan **Activity 23**. Final Report

8



6. PHASES & ACTIVITIES

Organization of Activities

Organization of the development of Activities in each of the Phases:

Phase 1 - DESIGN

1 Cybersecurity Literature Revision

2 Application Questionnaires

3 Desgin Framework V.1.0

4 Market Self-Assessment

Phase 2 - MARKET TEST

5 Taxonomy Threats and Attack Methods

6 Scenarios Threats and Attack Methods

7 Interviews Focus Groups Use Cases

8 Communication & Dissemination Plan

9 Desgin Framework V.2.0

10 Training & Awareness

11 Framework Support Application

12 Website

13 Market Self-Assessment

Phase 3 – CONCEPTION & APLICATION

14 Framework Application Process

15 Health Entities Application

16 Lessons Learned

17 Desgin Framework V.3.0

18 HISC4ALL Update

19 Market Validation + Website

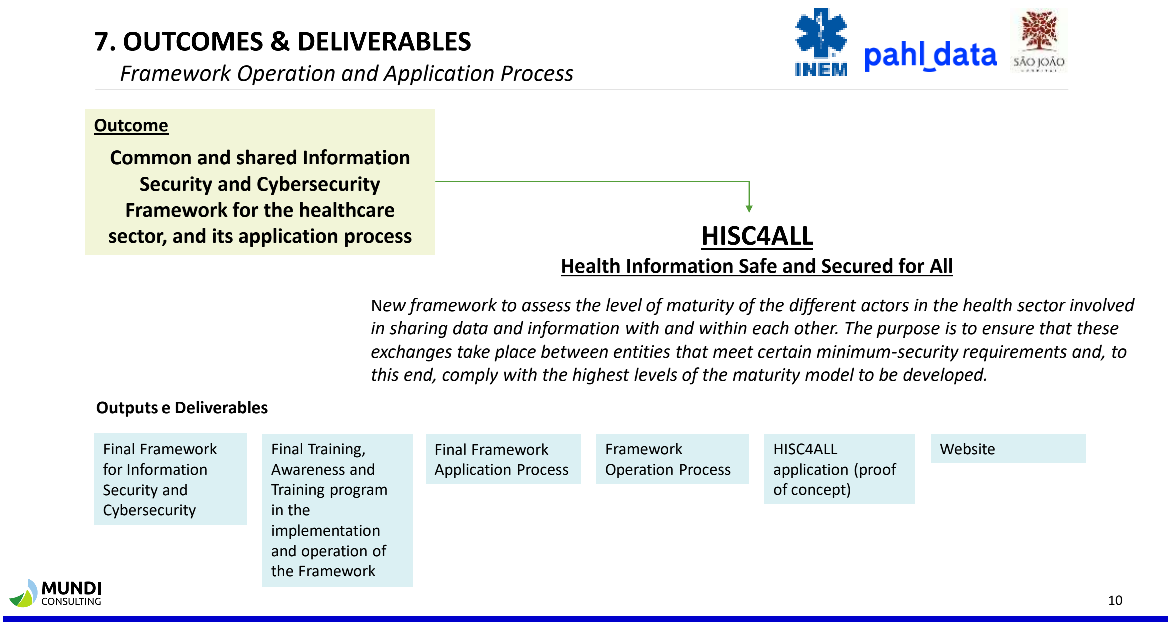
Phase 4 - DISSEMINATION

20 Availability of Framework HISC$ALL

21 Dissemination Pan + Website

22 Implementation Plan

23 Final Report



7. OUTCOMES & DELIVERABLES

Framework Operation and Application Process

Outcome

Common and shared Information Security and Cybersecurity Framework for the healthcare sector, and its application process

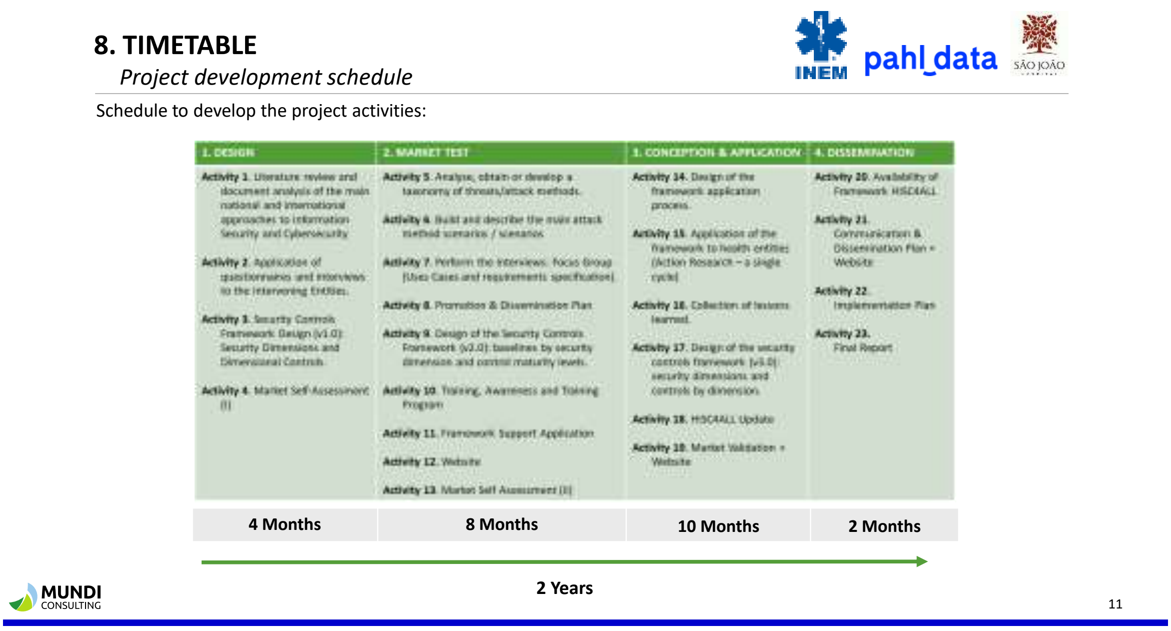
HISC4ALL

Health Information Safe and Secured for All

New framework to assess the level of maturity of the different actors in the health sector involved in sharing data and information with and within each other. The purpose is to ensure that these exchanges take place between entities that meet certain minimum-security requirements and, to this end, comply with the highest levels of the maturity model to be developed.

Outputs e Deliverables

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



8. TIMETABLE

Project development schedule

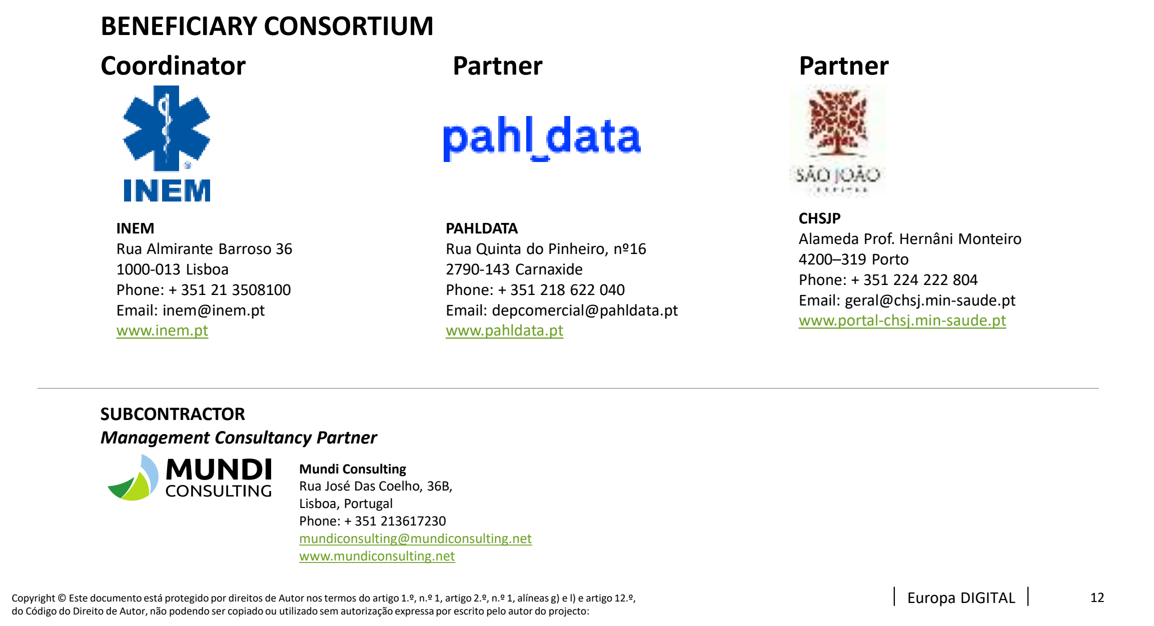
Schedule to develop the project activities:

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**. Promotion & Dissemination Plan **Activity 9**. Design of the Security Controls Framework (v2.0): baselines by security dimension and control maturity levels. **Activity 10**. Training, Awareness and Training Program **Activity 11**. Framework Support Application **Activity 12**. Website **Activity 13**. Market Self Assessment (II)	**Activity 14**. Design of the framework application process. **Activity 15**. Application of the framework to health entities (Action Research – a single cycle) **Activity 16**. Collection of lessons learned. **Activity 17**. Design of the security controls framework (v3.0): security dimensions and controls by dimension. **Activity 18**. HISC4ALL Update **Activity 19**. Market Validation + Website	**Activity 20**. Availability of Framework HISC4ALL **Activity 21**. Communication & Dissemination Plan + Website **Activity 22**. Implementation Plan **Activity 23**. Final Report
4 Months	8 Months	10 Months	2 Months

2 Years

MUNDI CONSULTING

11



BENEFICIARY CONSORTIUM

Coordinator

INEM
Rua Almirante Barroso 36
1000-013 Lisboa
Phone: + 351 21 3508100
Email: inem@inem.pt
www.inem.pt

Partner

PAHLDATA
Rua Quinta do Pinheiro, nº16
2790-143 Carnaxide
Phone: + 351 218 622 040
Email: depcomercial@pahldata.pt
www.pahldata.pt

Partner

CHSJP
Alameda Prof. Hernâni Monteiro
4200–319 Porto
Phone: + 351 224 222 804
Email: geral@chsj.min-saude.pt
www.portal-chsj.min-saude.pt

SUBCONTRACTOR

Management Consultancy Partner

Mundi Consulting
Rua José Das Coelho, 36B,
Lisboa, Portugal
Phone: + 351 213617230
mundiconsulting@mundiconsulting.net
www.mundiconsulting.net

Copyright © Este documento está protegido por direitos de Autor nos termos do artigo 1.º, n.º 1, artigo 2.º, n.º 1, alíneas g) e l) e artigo 12.º, do Código do Direito de Autor, não podendo ser copiado ou utilizado sem autorização expressa por escrito pelo autor do projecto:

Europa DIGITAL

12

HISTORY OF CHANGES		
VERSION	PUBLICATION DATE	CHANGE
1.0	23.09.2022	Initial version.
2.0	09.12.2022	Second version
3.0	31.10.2023	Third Version

DATA SHEET

1. General data

Project summary:

Project summary
The Project HISC4ALL – Health Information Safe and Secured for All, consist of creating a FRAMEWORK involving the SME in Design a common and shared Information Security and Cybersecurity Framework for the healthcare sector, and its application process. The promoters are Instituto Nacional de Emergência Médica (INEM)–Public Institution from the Ministry of Health, responsible for the Integrated Medical Emergency System; Hospital Lusíadas, Private Hospital; and QUATTRO–Private SME, Health Sector Information Solutions Provider. Covid-19 pandemic made a sudden and urgent shifted of the patient care to citizens' homes, making the Healthcare entities more exposed to cyber-attacks. The Consortium saw the need in the market to incorporate a Information Security and Cybersecurity tool. It gives to the market a personalized service of monitoring, detection, and response to security incidents, operated by a team of specialists, based on a set of technological solutions, and supported by standards and frameworks to ensure the compliance of the service. The Consortium propose to create a new framework to assess the level of maturity of the different actors in the health sector involved in sharing data and information with and within each other. The purpose is to ensure that these exchanges take place between entities that meet certain minimum-security requirements and, to this end, comply with the highest levels of the maturity model to be developed. Outcomes will be: 1)Final Framework for Information Security and Cybersecurity; 2)Final Training, Awareness and Training program in the implementation and operation of the Framework; 3)Final Framework Application Process; 4)Framework Operation Process; 5)HISC4ALL application (proof of concept); 6)Website. The target Stakeholders are 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).

Keywords:

- Cybersecurity Domains
- Cybersecurity
- Health data
- Trust
- Healthcare

Project number: 101100701

Project name: Health Information Safe and Cybersecured for All

Project acronym: HISC4ALL

Call: DIGITAL-2022-CYBER-02

Topic: DIGITAL-2022-CYBER-02-SUPPORTHEALTH

Type of action: Digital SME Support Actions

Granting authority: European Commission-EU

Grant managed through EU Funding & Tenders Portal: Yes (eGrants)

Project starting date: fixed date: 1 January 2023

Project end date: 31 December 2024

Project duration: 24 months

Consortium agreement: Yes

2. Participants

List of participants:

N°	Role	Short name	Legal name	Ctry	PIC	Total eligible costs (BEN and AE)	Max grant amount	Entry date	Exit date
1	COO	INEM	INEM	PT	940442840	380 959.59	190 479.00		
2	BEN	PAHLDATA	PAHLDATA (PORTUGAL) - COMERCIO DE EQUIPAMENTO DE INFORMATICA S.A.	PT	893426940	636 979.56	477 734.00		
3	BEN	CHSJP	CENTRO HOSPITALAR DE SAO JOAO EPE	PT	969128456	201 080.82	100 540.00	1/6/2023	
Total						1 219 019.97	768 753.00		

Coordinator:

– INEM (INEM): from 21 December 2022 to present

3. Grant

Maximum grant amount, total estimated eligible costs and contributions and funding rate:

Total eligible costs (BEN and AE)	Funding rate (%)	Maximum grant amount (Annex 2)	Maximum grant amount (award decision)
1 219 019.97	75, 50	768 753.00	768 753.00

Grant form: Budget-based

Grant mode: Action grant

Budget categories/activity types:

- A. Personnel costs
  - A.1 Employees, A.2 Natural persons under direct contract, A.3 Seconded persons
  - A.4 SME owners and natural person beneficiaries

- B. Subcontracting costs

- C. Purchase costs
  - C.1 Travel and subsistence
  - C.2 Equipment
  - C.3 Other goods, works and services

- D. Other cost categories
  - D.1 Financial support to third parties
  - D.2 Internally invoiced goods and services

- E. Indirect costs

Cost eligibility options:

- Standard supplementary payments

- Average personnel costs (unit cost according to usual cost accounting practices)

- Country restrictions for subcontracting costs

- Limitation for subcontracting

- Travel and subsistence:
  - Travel: Actual costs
  - Accommodation: Actual costs
  - Subsistence: Actual costs

- Equipment: depreciation only
- Costs for providing financial support to third parties (actual cost; max amount for each recipient: EUR 60 000.00)
- Indirect cost flat-rate: 7% of the eligible direct costs (categories A-D, except volunteers costs and exempted specific cost categories, if any)
- VAT: Yes
- Country restrictions for eligible costs
- Other ineligible costs

Budget flexibility: Yes (no flexibility cap)

4. Reporting, payments and recoveries

4.1 Continuous reporting (art 21)

Deliverables: see Funding & Tenders Portal Continuous Reporting tool

4.2 Periodic reporting and payments

Reporting and payment schedule (art 21, 22):

Reporting					Payments	
Reporting periods			Type	Deadline	Type	Deadline (time to pay)
RP No	Month from	Month to				
					Initial prefinancing	30 days from entry into force/10 days before starting date/ financial guarantee (if required) – whichever is the latest
1	1	12	Periodic report	60 days after end of reporting period	Interim payment	90 days from receiving periodic report
2	13	24	Periodic report	60 days after end of reporting period	Final payment	90 days from receiving periodic report

Prefinancing payments and guarantees:

Prefinancing payment		Prefinancing guarantee		
Type	Amount	Guarantee amount	Division per participant	
Prefinancing 1 (initial)	615 002.40	n/a	1 - INEM	n/a
			2 - PAHLDATA	n/a
			3 - CHSJP	n/a

Reporting and payment modalities (art 21, 22):

Mutual Insurance Mechanism (MIM): No

Restrictions on distribution of initial prefinancing: The prefinancing may be distributed only if the minimum number of beneficiaries set out in the call condititions (if any) have acceded to the Agreement and only to beneficiaries that have acceded.

Interim payment ceiling (if any): 90% of the maximum grant amount

No-profit rule: Yes

Late payment interest: ECB + 3.5%

Bank account for payments:

PT50078101120000000789942

Conversion into euros: Double conversion

Reporting language: Language of the Agreement

4.3 Certificates (art 24):

Certificates on the financial statements (CFS):

Conditions:

Schedule: only at final payment, if threshold is reached

Standard threshold (beneficiary-level):

- financial statement: requested EU contribution to costs ≥ EUR 325 000.00

4.4 Recoveries (art 22)

First-line liability for recoveries:

Beneficiary termination: Beneficiary concerned

Final payment: Coordinator

After final payment: Beneficiary concerned

Joint and several liability for enforced recoveries (in case of non-payment):

Limited joint and several liability of other beneficiaries — up to the maximum grant amount of the beneficiary

Joint and several liability of affiliated entities — n/a

5. Consequences of non-compliance, applicable law & dispute settlement forum

Applicable law (art 43):

Standard applicable law regime: EU law + law of Belgium

Dispute settlement forum (art 43):

Standard dispute settlement forum:

EU beneficiaries: EU General Court + EU Court of Justice (on appeal)

Non-EU beneficiaries: Courts of Brussels, Belgium (unless an international agreement provides for the enforceability of EU court judgements)

6. Other

Specific rules (Annex 5): Yes

Standard time-limits after project end:

Confidentiality (for X years after final payment): 5

Record-keeping (for X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)

Reviews (up to X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)

Audits (up to X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)

Extension of findings from other grants to this grant (no later than X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)

Impact evaluation (up to X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)