



EUROPEAN COMMISSION
Directorate-General for Communications Networks, Content and Technology
CNECT.H – Digital Society, Trust and Cybersecurity
H.1 – Cybersecurity Technology and Capacity Building

GRANT AGREEMENT

Project 101100701 — HISC4ALL

PREAMBLE

This **Agreement** (‘the Agreement’) is **between** the following parties:

on the one part,

the **European Union** (‘EU’), represented by the European Commission (‘European Commission’ or ‘granting authority’),

and

on the other part,

1. ‘the coordinator’:

INEM (INEM), PIC 940442840, established in RUE ALMIRANTE BARROSO 36, LISBON 1000 013, Portugal,

and the following other beneficiaries, if they sign their ‘accession form’ (see Annex 3 and Article 40):

2. **PAHLDATA (PORTUGAL) - COMERCIO DE EQUIPAMENTO DE INFORMATICA S.A. (PAHLDATA)**, PIC 893426940, established in RUA QUINTA DO PINHEIRO N 16-3 C, CARNAXIDE 2790-143, Portugal,

Unless otherwise specified, references to ‘beneficiary’ or ‘beneficiaries’ include the coordinator and affiliated entities (if any).

If only one beneficiary signs the grant agreement (‘mono-beneficiary grant’), all provisions referring to the ‘coordinator’ or the ‘beneficiaries’ will be considered — mutatis mutandis — as referring to the beneficiary.

The parties referred to above have agreed to enter into the Agreement.

By signing the Agreement and the accession forms, the beneficiaries accept the grant and agree to implement the action under their own responsibility and in accordance with the Agreement, with all the obligations and terms and conditions it sets out.

The Agreement is composed of:

Preamble

Terms and Conditions (including Data Sheet)

Annex 1 Description of the action¹

Annex 2 Estimated budget for the action

Annex 2a Additional information on unit costs and contributions (if applicable)

Annex 3 Accession forms (if applicable)²

Annex 3a Declaration on joint and several liability of affiliated entities (if applicable)³

Annex 4 Model for the financial statements

Annex 5 Specific rules (if applicable)

¹ Template published on [Portal Reference Documents](#).

² Template published on [Portal Reference Documents](#).

³ Template published on [Portal Reference Documents](#).

TERMS AND CONDITIONS

TABLE OF CONTENTS

GRANT AGREEMENT.....	1
PREAMBLE.....	1
TERMS AND CONDITIONS.....	3
DATASHEET.....	8
CHAPTER 1 GENERAL.....	13
ARTICLE 1 — SUBJECT OF THE AGREEMENT	13
ARTICLE 2 — DEFINITIONS.....	13
CHAPTER 2 ACTION.....	14
ARTICLE 3 — ACTION.....	14
ARTICLE 4 — DURATION AND STARTING DATE.....	14
CHAPTER 3 GRANT.....	14
ARTICLE 5 — GRANT.....	14
5.1 Form of grant.....	14
5.2 Maximum grant amount.....	15
5.3 Funding rate.....	15
5.4 Estimated budget, budget categories and forms of funding.....	15
5.5 Budget flexibility.....	15
ARTICLE 6 — ELIGIBLE AND INELIGIBLE COSTS AND CONTRIBUTIONS.....	16
6.1 General eligibility conditions.....	16
6.2 Specific eligibility conditions for each budget category.....	17
6.3 Ineligible costs and contributions.....	21
6.4 Consequences of non-compliance.....	23
CHAPTER 4 GRANT IMPLEMENTATION.....	23
SECTION 1 CONSORTIUM: BENEFICIARIES, AFFILIATED ENTITIES AND OTHER PARTICIPANTS.....	23
ARTICLE 7 — BENEFICIARIES.....	23
ARTICLE 8 — AFFILIATED ENTITIES.....	25
ARTICLE 9 — OTHER PARTICIPANTS INVOLVED IN THE ACTION.....	25
9.1 Associated partners.....	25
9.2 Third parties giving in-kind contributions to the action.....	25
9.3 Subcontractors.....	25

9.4 Recipients of financial support to third parties.....	26
ARTICLE 10 — PARTICIPANTS WITH SPECIAL STATUS.....	26
10.1 Non-EU participants.....	26
10.2 Participants which are international organisations.....	26
10.3 Pillar-assessed participants.....	27
SECTION 2 RULES FOR CARRYING OUT THE ACTION.....	29
ARTICLE 11 — PROPER IMPLEMENTATION OF THE ACTION.....	29
11.1 Obligation to properly implement the action.....	29
11.2 Consequences of non-compliance.....	29
ARTICLE 12 — CONFLICT OF INTERESTS.....	29
12.1 Conflict of interests.....	29
12.2 Consequences of non-compliance.....	30
ARTICLE 13 — CONFIDENTIALITY AND SECURITY.....	30
13.1 Sensitive information.....	30
13.2 Classified information.....	30
13.3 Consequences of non-compliance.....	31
ARTICLE 14 — ETHICS AND VALUES.....	31
14.1 Ethics.....	31
14.2 Values.....	31
14.3 Consequences of non-compliance.....	31
ARTICLE 15 — DATA PROTECTION.....	31
15.1 Data processing by the granting authority.....	31
15.2 Data processing by the beneficiaries.....	32
15.3 Consequences of non-compliance.....	32
ARTICLE 16 — INTELLECTUAL PROPERTY RIGHTS (IPR) — BACKGROUND AND RESULTS — ACCESS RIGHTS AND RIGHTS OF USE.....	32
16.1 Background and access rights to background.....	33
16.2 Ownership of results.....	33
16.3 Rights of use of the granting authority on materials, documents and information received for policy, information, communication, dissemination and publicity purposes.....	33
16.4 Specific rules on IPR, results and background.....	34
16.5 Consequences of non-compliance.....	34
ARTICLE 17 — COMMUNICATION, DISSEMINATION AND VISIBILITY.....	34
17.1 Communication — Dissemination — Promoting the action.....	34
17.2 Visibility — European flag and funding statement.....	34
17.3 Quality of information — Disclaimer.....	35

17.4	Specific communication, dissemination and visibility rules.....	35
17.5	Consequences of non-compliance.....	36
ARTICLE 18 — SPECIFIC RULES FOR CARRYING OUT THE ACTION.....		36
18.1	Specific rules for carrying out the action.....	36
18.2	Consequences of non-compliance.....	36
SECTION 3 GRANT ADMINISTRATION.....		36
ARTICLE 19 — GENERAL INFORMATION OBLIGATIONS.....		36
19.1	Information requests.....	36
19.2	Participant Register data updates.....	36
19.3	Information about events and circumstances which impact the action.....	36
19.4	Consequences of non-compliance.....	37
ARTICLE 20 — RECORD-KEEPING.....		37
20.1	Keeping records and supporting documents.....	37
20.2	Consequences of non-compliance.....	38
ARTICLE 21 — REPORTING.....		38
21.1	Continuous reporting.....	38
21.2	Periodic reporting: Technical reports and financial statements.....	38
21.3	Currency for financial statements and conversion into euros.....	39
21.4	Reporting language.....	40
21.5	Consequences of non-compliance.....	40
ARTICLE 22 — PAYMENTS AND RECOVERIES — CALCULATION OF AMOUNTS DUE.....		40
22.1	Payments and payment arrangements.....	40
22.2	Recoveries.....	40
22.3	Amounts due.....	41
22.4	Enforced recovery.....	45
22.5	Consequences of non-compliance.....	46
ARTICLE 23 — GUARANTEES.....		47
23.1	Prefinancing guarantee.....	47
23.2	Consequences of non-compliance.....	47
ARTICLE 24 — CERTIFICATES.....		47
24.1	Operational verification report (OVR).....	47
24.2	Certificate on the financial statements (CFS).....	47
24.3	Certificate on the compliance of usual cost accounting practices (CoMUC).....	48
24.4	Systems and process audit (SPA).....	48
24.5	Consequences of non-compliance.....	49

ARTICLE 25 — CHECKS, REVIEWS, AUDITS AND INVESTIGATIONS — EXTENSION OF FINDINGS.....	49
25.1 Granting authority checks, reviews and audits.....	49
25.2 European Commission checks, reviews and audits in grants of other granting authorities.....	50
25.3 Access to records for assessing simplified forms of funding.....	50
25.4 OLAF, EPPO and ECA audits and investigations.....	50
25.5 Consequences of checks, reviews, audits and investigations — Extension of results of reviews, audits or investigations.....	51
25.6 Consequences of non-compliance.....	52
ARTICLE 26 — IMPACT EVALUATIONS.....	52
26.1 Impact evaluation.....	52
26.2 Consequences of non-compliance.....	53
CHAPTER 5 CONSEQUENCES OF NON-COMPLIANCE.....	53
SECTION 1 REJECTIONS AND GRANT REDUCTION.....	53
ARTICLE 27 — REJECTION OF COSTS AND CONTRIBUTIONS.....	53
27.1 Conditions.....	53
27.2 Procedure.....	53
27.3 Effects.....	53
ARTICLE 28 — GRANT REDUCTION.....	53
28.1 Conditions.....	53
28.2 Procedure.....	54
28.3 Effects.....	54
SECTION 2 SUSPENSION AND TERMINATION.....	54
ARTICLE 29 — PAYMENT DEADLINE SUSPENSION.....	54
29.1 Conditions.....	54
29.2 Procedure.....	55
ARTICLE 30 — PAYMENT SUSPENSION.....	55
30.1 Conditions.....	55
30.2 Procedure.....	55
ARTICLE 31 — GRANT AGREEMENT SUSPENSION.....	56
31.1 Consortium-requested GA suspension.....	56
31.2 EU-initiated GA suspension.....	57
ARTICLE 32 — GRANT AGREEMENT OR BENEFICIARY TERMINATION.....	58
32.1 Consortium-requested GA termination.....	58
32.2 Consortium-requested beneficiary termination.....	59
32.3 EU-initiated GA or beneficiary termination.....	60

SECTION 3 OTHER CONSEQUENCES: DAMAGES AND ADMINISTRATIVE SANCTIONS..... 63

ARTICLE 33 — DAMAGES..... 63

 33.1 Liability of the granting authority..... 63

 33.2 Liability of the beneficiaries..... 63

ARTICLE 34 — ADMINISTRATIVE SANCTIONS AND OTHER MEASURES..... 64

SECTION 4 FORCE MAJEURE..... 64

ARTICLE 35 — FORCE MAJEURE..... 64

CHAPTER 6 FINAL PROVISIONS..... 64

ARTICLE 36 — COMMUNICATION BETWEEN THE PARTIES..... 64

 36.1 Forms and means of communication — Electronic management..... 64

 36.2 Date of communication..... 65

 36.3 Addresses for communication..... 65

ARTICLE 37 — INTERPRETATION OF THE AGREEMENT..... 65

ARTICLE 38 — CALCULATION OF PERIODS AND DEADLINES..... 65

ARTICLE 39 — AMENDMENTS..... 66

 39.1 Conditions..... 66

 39.2 Procedure..... 66

ARTICLE 40 — ACCESSION AND ADDITION OF NEW BENEFICIARIES..... 66

 40.1 Accession of the beneficiaries mentioned in the Preamble..... 67

 40.2 Addition of new beneficiaries..... 67

ARTICLE 41 — TRANSFER OF THE AGREEMENT..... 67

ARTICLE 42 — ASSIGNMENTS OF CLAIMS FOR PAYMENT AGAINST THE GRANTING
AUTHORITY..... 67

ARTICLE 43 — APPLICABLE LAW AND SETTLEMENT OF DISPUTES..... 68

 43.1 Applicable law..... 68

 43.2 Dispute settlement..... 68

ARTICLE 44 — ENTRY INTO FORCE..... 68

DATA SHEET

1. General data

Project summary:

Project summary
<p>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).</p>

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:

Nº	Role	Short name	Legal name	Ctry	PIC	Total eligible costs (BEN and AE)	Max grant amount
1	COO	INEM	INEM	PT	940442840	582 040.41	291 019.00
2	BEN	PAHLDATA	PAHLDATA (PORTUGAL) - COMERCIO DE EQUIPAMENTO DE INFORMATICA S.A.	PT	893426940	636 979.56	477 734.00
Total						1 219 019.97	768 753.00

Coordinator:

- INEM (INEM)

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)
- 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

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 conditions (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 \geq 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)

CHAPTER 1 GENERAL

ARTICLE 1 — SUBJECT OF THE AGREEMENT

This Agreement sets out the rights and obligations and terms and conditions applicable to the grant awarded for the implementation of the action set out in Chapter 2.

ARTICLE 2 — DEFINITIONS

For the purpose of this Agreement, the following definitions apply:

Actions — The project which is being funded in the context of this Agreement.

Grant — The grant awarded in the context of this Agreement.

EU grants — Grants awarded by EU institutions, bodies, offices or agencies (including EU executive agencies, EU regulatory agencies, EDA, joint undertakings, etc.).

Participants — Entities participating in the action as beneficiaries, affiliated entities, associated partners, third parties giving in-kind contributions, subcontractors or recipients of financial support to third parties.

Beneficiaries (BEN) — The signatories of this Agreement (either directly or through an accession form).

Affiliated entities (AE) — Entities affiliated to a beneficiary within the meaning of Article 187 of EU Financial Regulation 2018/1046⁴ which participate in the action with similar rights and obligations as the beneficiaries (obligation to implement action tasks and right to charge costs and claim contributions).

Associated partners (AP) — Entities which participate in the action, but without the right to charge costs or claim contributions.

Purchases — Contracts for goods, works or services needed to carry out the action (e.g. equipment, consumables and supplies) but which are not part of the action tasks (see Annex 1).

Subcontracting — Contracts for goods, works or services that are part of the action tasks (see Annex 1).

In-kind contributions — In-kind contributions within the meaning of Article 2(36) of EU Financial

⁴ For the definition, see Article 187 Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 ('EU Financial Regulation') (OJ L 193, 30.7.2018, p. 1): "**affiliated entities** [are]:

- (a) entities that form a sole beneficiary [(i.e. where an entity is formed of several entities that satisfy the criteria for being awarded a grant, including where the entity is specifically established for the purpose of implementing an action to be financed by a grant)];
- (b) entities that satisfy the eligibility criteria and that do not fall within one of the situations referred to in Article 136(1) and 141(1) and that have a link with the beneficiary, in particular a legal or capital link, which is neither limited to the action nor established for the sole purpose of its implementation".

Regulation 2018/1046, i.e. non-financial resources made available free of charge by third parties.

Fraud — Fraud within the meaning of Article 3 of EU Directive 2017/1371⁵ and Article 1 of the Convention on the protection of the European Communities' financial interests, drawn up by the Council Act of 26 July 1995⁶, as well as any other wrongful or criminal deception intended to result in financial or personal gain.

Irregularities — Any type of breach (regulatory or contractual) which could impact the EU financial interests, including irregularities within the meaning of Article 1(2) of EU Regulation 2988/95⁷.

Grave professional misconduct — Any type of unacceptable or improper behaviour in exercising one's profession, especially by employees, including grave professional misconduct within the meaning of Article 136(1)(c) of EU Financial Regulation 2018/1046.

Applicable EU, international and national law — Any legal acts or other (binding or non-binding) rules and guidance in the area concerned.

Portal — EU Funding & Tenders Portal; electronic portal and exchange system managed by the European Commission and used by itself and other EU institutions, bodies, offices or agencies for the management of their funding programmes (grants, procurements, prizes, etc.).

CHAPTER 2 ACTION

ARTICLE 3 — ACTION

The grant is awarded for the action **101100701 — HISC4ALL** ('action'), as described in Annex 1.

ARTICLE 4 — DURATION AND STARTING DATE

The duration and the starting date of the action are set out in the Data Sheet (see Point 1).

CHAPTER 3 GRANT

ARTICLE 5 — GRANT

5.1 Form of grant

The grant is an action grant⁸ which takes the form of a budget-based mixed actual cost grant (i.e. a

⁵ Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law (OJ L 198, 28.7.2017, p. 29).

⁶ OJ C 316, 27.11.1995, p. 48.

⁷ Council Regulation (EC, Euratom) No 2988/95 of 18 December 1995 on the protection of the European Communities financial interests (OJ L 312, 23.12.1995, p. 1).

⁸ For the definition, see Article 180(2)(a) EU Financial Regulation 2018/1046: '**action grant**' means an EU grant to finance "an action intended to help achieve a Union policy objective".

grant based on actual costs incurred, but which may also include other forms of funding, such as unit costs or contributions, flat-rate costs or contributions, lump sum costs or contributions or financing not linked to costs).

5.2 Maximum grant amount

The maximum grant amount is set out in the Data Sheet (see Point 3) and in the estimated budget (Annex 2).

5.3 Funding rate

The funding rate for costs is 75% of the eligible costs for beneficiaries that are SMEs and 50% of the eligible costs for other beneficiaries.

Contributions are not subject to any funding rate.

5.4 Estimated budget, budget categories and forms of funding

The estimated budget for the action is set out in Annex 2.

It contains the estimated eligible costs and contributions for the action, broken down by participant and budget category.

Annex 2 also shows the types of costs and contributions (forms of funding)⁹ to be used for each budget category.

If unit costs or contributions are used, the details on the calculation will be explained in Annex 2a.

5.5 Budget flexibility

The budget breakdown may be adjusted — without an amendment (see Article 39) — by transfers (between participants and budget categories), as long as this does not imply any substantive or important change to the description of the action in Annex 1.

However:

- changes to the budget category for volunteers (if used) always require an amendment
- changes to budget categories with lump sums costs or contributions (if used; including financing not linked to costs) always require an amendment
- changes to budget categories with higher funding rates or budget ceilings (if used) always require an amendment
- addition of amounts for subcontracts not provided for in Annex 1 either require an amendment or simplified approval in accordance with Article 6.2
- other changes require an amendment or simplified approval, if specifically provided for in Article 6.2

⁹ See Article 125 EU Financial Regulation 2018/1046.

- flexibility caps: not applicable.

ARTICLE 6 — ELIGIBLE AND INELIGIBLE COSTS AND CONTRIBUTIONS

In order to be eligible, costs and contributions must meet the **eligibility** conditions set out in this Article.

6.1 General eligibility conditions

The **general eligibility conditions** are the following:

- (a) for actual costs:
 - (i) they must be actually incurred by the beneficiary
 - (ii) they must be incurred in the period set out in Article 4 (with the exception of costs relating to the submission of the final periodic report, which may be incurred afterwards; see Article 21)
 - (iii) they must be declared under one of the budget categories set out in Article 6.2 and Annex 2
 - (iv) they must be incurred in connection with the action as described in Annex 1 and necessary for its implementation
 - (v) they must be identifiable and verifiable, in particular recorded in the beneficiary's accounts in accordance with the accounting standards applicable in the country where the beneficiary is established and with the beneficiary's usual cost accounting practices
 - (vi) they must comply with the applicable national law on taxes, labour and social security and
 - (vii) they must be reasonable, justified and must comply with the principle of sound financial management, in particular regarding economy and efficiency
- (b) for unit costs or contributions (if any):
 - (i) they must be declared under one of the budget categories set out in Article 6.2 and Annex 2
 - (ii) the units must:
 - be actually used or produced by the beneficiary in the period set out in Article 4 (with the exception of units relating to the submission of the final periodic report, which may be used or produced afterwards; see Article 21)
 - be necessary for the implementation of the action and
 - (iii) the number of units must be identifiable and verifiable, in particular supported by records and documentation (see Article 20)
- (c) for flat-rate costs or contributions (if any):

- (i) they must be declared under one of the budget categories set out in Article 6.2 and Annex 2
- (ii) the costs or contributions to which the flat-rate is applied must:
 - be eligible
 - relate to the period set out in Article 4 (with the exception of costs or contributions relating to the submission of the final periodic report, which may be incurred afterwards; see Article 21)
- (d) for lump sum costs or contributions (if any):
 - (i) they must be declared under one of the budget categories set out in Article 6.2 and Annex 2
 - (ii) the work must be properly implemented by the beneficiary in accordance with Annex 1
 - (iii) the deliverables/outputs must be achieved in the period set out in Article 4 (with the exception of deliverables/outputs relating to the submission of the final periodic report, which may be achieved afterwards; see Article 21)
- (e) for unit, flat-rate or lump sum costs or contributions according to usual cost accounting practices (if any):
 - (i) they must fulfil the general eligibility conditions for the type of cost concerned
 - (ii) the cost accounting practices must be applied in a consistent manner, based on objective criteria, regardless of the source of funding
- (f) for financing not linked to costs (if any): the results must be achieved or the conditions must be fulfilled as described in Annex 1.

In addition, for direct cost categories (e.g. personnel, travel & subsistence, subcontracting and other direct costs) only costs that are directly linked to the action implementation and can therefore be attributed to it directly are eligible. They must not include any indirect costs (i.e. costs that are only indirectly linked to the action, e.g. via cost drivers).

6.2 Specific eligibility conditions for each budget category

For each budget category, the **specific eligibility conditions** are as follows:

Direct costs

A. Personnel costs

A.1 Costs for employees (or equivalent) are eligible as personnel costs if they fulfil the general eligibility conditions and are related to personnel working for the beneficiary under an employment contract (or equivalent appointing act) and assigned to the action.

They must be limited to salaries, social security contributions, taxes and other costs linked to the remuneration, if they arise from national law or the employment contract (or equivalent appointing

act) and be calculated on the basis of the costs actually incurred, in accordance with the following method:

{daily rate for the person
multiplied by
number of day-equivalents worked on the action (rounded up or down to the nearest half-day)}.

The daily rate must be calculated as:

{annual personnel costs for the person
divided by
215}.

The number of day-equivalents declared for a person must be identifiable and verifiable (see Article 20).

The total number of day-equivalents declared in EU grants, for a person for a year, cannot be higher than 215.

The personnel costs may also include supplementary payments for personnel assigned to the action (including payments on the basis of supplementary contracts regardless of their nature), if:

- it is part of the beneficiary's usual remuneration practices and is paid in a consistent manner whenever the same kind of work or expertise is required
- the criteria used to calculate the supplementary payments are objective and generally applied by the beneficiary, regardless of the source of funding used.

If the beneficiary uses average personnel costs (unit cost according to usual cost accounting practices), the personnel costs must fulfil the general eligibility conditions for such unit costs and the daily rate must be calculated:

- using the actual personnel costs recorded in the beneficiary's accounts and excluding any costs which are ineligible or already included in other budget categories; the actual personnel costs may be adjusted on the basis of budgeted or estimated elements, if they are relevant for calculating the personnel costs, reasonable and correspond to objective and verifiable information

and

- according to usual cost accounting practices which are applied in a consistent manner, based on objective criteria, regardless of the source of funding.

A.2 and A.3 Costs for natural persons working under a direct contract other than an employment contract and costs for **seconded persons by a third party against payment** are also eligible as personnel costs, if they are assigned to the action, fulfil the general eligibility conditions and:

- (a) work under conditions similar to those of an employee (in particular regarding the way the work is organised, the tasks that are performed and the premises where they are performed) and
- (b) the result of the work belongs to the beneficiary (unless agreed otherwise).

They must be calculated on the basis of a rate which corresponds to the costs actually incurred for the direct contract or secondment and must not be significantly different from those for personnel performing similar tasks under an employment contract with the beneficiary.

A.4 The work of **SME owners** for the action (i.e. owners of beneficiaries that are small and medium-sized enterprises¹⁰ not receiving a salary) or **natural person beneficiaries** (i.e. beneficiaries that are natural persons not receiving a salary) may be declared as personnel costs, if they fulfil the general eligibility conditions and are calculated as unit costs in accordance with the method set out in Annex 2a.

B. Subcontracting costs

Subcontracting costs for the action (including related duties, taxes and charges, such as non-deductible or non-refundable value added tax (VAT)) are eligible, if they are calculated on the basis of the costs actually incurred, fulfil the general eligibility conditions and are awarded using the beneficiary's usual purchasing practices — provided these ensure subcontracts with best value for money (or if appropriate the lowest price) and that there is no conflict of interests (see Article 12).

Beneficiaries that are 'contracting authorities/entities' within the meaning of the EU Directives on public procurement must also comply with the applicable national law on public procurement.

The beneficiaries must ensure that the subcontracted work is performed in the eligible countries or target countries set out in the call conditions — unless otherwise approved by the granting authority.

Subcontracting may cover only a limited part of the action.

The tasks to be subcontracted and the estimated cost for each subcontract must be set out in Annex 1 and the total estimated costs of subcontracting per beneficiary must be set out in Annex 2 (or may be approved ex post in the periodic report, if the use of subcontracting does not entail changes to the Agreement which would call into question the decision awarding the grant or breach the principle of equal treatment of applicants; 'simplified approval procedure').

C. Purchase costs

Purchase costs for the action (including related duties, taxes and charges, such as non-deductible or non-refundable value added tax (VAT)) are eligible if they fulfil the general eligibility conditions and are bought using the beneficiary's usual purchasing practices — provided these ensure purchases with best value for money (or if appropriate the lowest price) and that there is no conflict of interests (see Article 12).

¹⁰ For the definition, see Commission Recommendation 2003/361/EC: micro, small or medium-sized enterprise (SME) are enterprises

- engaged in an economic activity, irrespective of their legal form (including, in particular, self-employed persons and family businesses engaged in craft or other activities, and partnerships or associations regularly engaged in an economic activity) and
- employing fewer than 250 persons (expressed in 'annual working units' as defined in Article 5 of the Recommendation) and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.

Beneficiaries that are ‘contracting authorities/entities’ within the meaning of the EU Directives on public procurement must also comply with the applicable national law on public procurement.

C.1 Travel and subsistence

Purchases for **travel, accommodation and subsistence** must be calculated as follows:

- travel: on the basis of the costs actually incurred and in line with the beneficiary’s usual practices on travel
- accommodation: on the basis of the costs actually incurred and in line with the beneficiary’s usual practices on travel
- subsistence: on the basis of the costs actually incurred and in line with the beneficiary’s usual practices on travel .

C.2 Equipment

Purchases of **equipment, infrastructure or other assets** used for the action must be declared as depreciation costs, calculated on the basis of the costs actually incurred and written off in accordance with international accounting standards and the beneficiary’s usual accounting practices.

Only the portion of the costs that corresponds to the rate of actual use for the action during the action duration can be taken into account.

Costs for **renting or leasing** equipment, infrastructure or other assets are also eligible, if they do not exceed the depreciation costs of similar equipment, infrastructure or assets and do not include any financing fees.

C.3 Other goods, works and services

Purchases of **other goods, works and services** must be calculated on the basis of the costs actually incurred.

Such goods, works and services include, for instance, consumables and supplies, promotion, dissemination, protection of results, translations, publications, certificates and financial guarantees, if required under the Agreement.

D. Other cost categories

D.1 Financial support to third parties

Costs for providing financial support to third parties (in the form of **grants, prizes** or similar forms of support; if any) are eligible, if and as declared eligible in the call conditions, if they fulfil the general eligibility conditions, are calculated on the basis of the costs actually incurred and the support is implemented in accordance with the conditions set out in Annex 1.

These conditions must ensure objective and transparent selection procedures and include at least the following:

- (a) for grants (or similar):
 - (i) the maximum amount of financial support for each third party (‘recipient’); this amount

may not exceed the amount set out in the Data Sheet (see Point 3) or otherwise agreed with the granting authority

- (ii) the criteria for calculating the exact amount of the financial support
 - (iii) the different types of activity that qualify for financial support, on the basis of a closed list
 - (iv) the persons or categories of persons that will be supported and
 - (v) the criteria and procedures for giving financial support
- (b) for prizes (or similar):
- (i) the eligibility and award criteria
 - (ii) the amount of the prize and
 - (iii) the payment arrangements.

D.2 Internally invoiced goods and services

Costs for internally invoiced goods and services directly used for the action may be declared as unit cost according to usual cost accounting practices, if and as declared eligible in the call conditions, if they fulfil the general eligibility conditions for such unit costs and the amount per unit is calculated:

- using the actual costs for the good or service recorded in the beneficiary's accounts, attributed either by direct measurement or on the basis of cost drivers, and excluding any cost which are ineligible or already included in other budget categories; the actual costs may be adjusted on the basis of budgeted or estimated elements, if they are relevant for calculating the costs, reasonable and correspond to objective and verifiable information

and

- according to usual cost accounting practices which are applied in a consistent manner, based on objective criteria, regardless of the source of funding.

'Internally invoiced goods and services' means goods or services which are provided within the beneficiary's organisation directly for the action and which the beneficiary values on the basis of its usual cost accounting practices.

Indirect costs

E. Indirect costs

Indirect costs will be reimbursed at the flat-rate of 7% of the eligible direct costs (categories A-D, except volunteers costs and exempted specific cost categories, if any).

Contributions

Not applicable

6.3 Ineligible costs and contributions

The following costs or contributions are **ineligible**:

- (a) costs or contributions that do not comply with the conditions set out above (Article 6.1 and 6.2), in particular:
 - (i) costs related to return on capital and dividends paid by a beneficiary
 - (ii) debt and debt service charges
 - (iii) provisions for future losses or debts
 - (iv) interest owed
 - (v) currency exchange losses
 - (vi) bank costs charged by the beneficiary's bank for transfers from the granting authority
 - (vii) excessive or reckless expenditure
 - (viii) deductible or refundable VAT (including VAT paid by public bodies acting as public authority)
 - (ix) costs incurred or contributions for activities implemented during grant agreement suspension (see Article 31)
 - (x) in-kind contributions by third parties
- (b) costs or contributions declared under other EU grants (or grants awarded by an EU Member State, non-EU country or other body implementing the EU budget), except for the following cases:
 - (i) Synergy actions: not applicable
 - (ii) if the action grant is combined with an operating grant¹¹ running during the same period and the beneficiary can demonstrate that the operating grant does not cover any (direct or indirect) costs of the action grant
- (c) costs or contributions for staff of a national (or regional/local) administration, for activities that are part of the administration's normal activities (i.e. not undertaken only because of the grant)
- (d) costs or contributions (especially travel and subsistence) for staff or representatives of EU institutions, bodies or agencies
- (e) other :
 - (i) costs or contributions for activities that do not take place in one of the eligible countries or target countries set out in the call conditions — unless approved by the granting authority
 - (ii) costs or contributions declared specifically ineligible in the call conditions.

¹¹ For the definition, see Article 180(2)(b) of EU Financial Regulation 2018/1046: '**operating grant**' means an EU grant to finance "the functioning of a body which has an objective forming part of and supporting an EU policy".

6.4 Consequences of non-compliance

If a beneficiary declares costs or contributions that are ineligible, they will be rejected (see Article 27).

This may also lead to other measures described in Chapter 5.

CHAPTER 4 GRANT IMPLEMENTATION

SECTION 1 CONSORTIUM: BENEFICIARIES, AFFILIATED ENTITIES AND OTHER PARTICIPANTS

ARTICLE 7 — BENEFICIARIES

The beneficiaries, as signatories of the Agreement, are fully responsible towards the granting authority for implementing it and for complying with all its obligations.

They must implement the Agreement to their best abilities, in good faith and in accordance with all the obligations and terms and conditions it sets out.

They must have the appropriate resources to implement the action and implement the action under their own responsibility and in accordance with Article 11. If they rely on affiliated entities or other participants (see Articles 8 and 9), they retain sole responsibility towards the granting authority and the other beneficiaries.

They are jointly responsible for the *technical* implementation of the action. If one of the beneficiaries fails to implement their part of the action, the other beneficiaries must ensure that this part is implemented by someone else (without being entitled to an increase of the maximum grant amount and subject to an amendment; see Article 39). The *financial* responsibility of each beneficiary in case of recoveries is governed by Article 22.

The beneficiaries (and their action) must remain eligible under the EU programme funding the grant for the entire duration of the action. Costs and contributions will be eligible only as long as the beneficiary and the action are eligible.

The **internal roles and responsibilities** of the beneficiaries are divided as follows:

- (a) Each beneficiary must:
 - (i) keep information stored in the Portal Participant Register up to date (see Article 19)
 - (ii) inform the granting authority (and the other beneficiaries) immediately of any events or circumstances likely to affect significantly or delay the implementation of the action (see Article 19)
 - (iii) submit to the coordinator in good time:
 - the prefinancing guarantees (if required; see Article 23)
 - the financial statements and certificates on the financial statements (CFS) (if required; see Articles 21 and 24.2 and Data Sheet, Point 4.3)

- the contribution to the deliverables and technical reports (see Article 21)
 - any other documents or information required by the granting authority under the Agreement
- (iv) submit via the Portal data and information related to the participation of their affiliated entities.
- (b) The coordinator must:
- (i) monitor that the action is implemented properly (see Article 11)
 - (ii) act as the intermediary for all communications between the consortium and the granting authority, unless the Agreement or granting authority specifies otherwise, and in particular:
 - submit the prefinancing guarantees to the granting authority (if any)
 - request and review any documents or information required and verify their quality and completeness before passing them on to the granting authority
 - submit the deliverables and reports to the granting authority
 - inform the granting authority about the payments made to the other beneficiaries (report on the distribution of payments; if required, see Articles 22 and 32)
 - (iii) distribute the payments received from the granting authority to the other beneficiaries without unjustified delay (see Article 22).

The coordinator may not delegate or subcontract the above-mentioned tasks to any other beneficiary or third party (including affiliated entities).

However, coordinators which are public bodies may delegate the tasks set out in Point (b)(ii) last indent and (iii) above to entities with ‘authorisation to administer’ which they have created or which are controlled by or affiliated to them. In this case, the coordinator retains sole responsibility for the payments and for compliance with the obligations under the Agreement.

Moreover, coordinators which are ‘sole beneficiaries’¹² (or similar, such as European research infrastructure consortia (ERICs)) may delegate the tasks set out in Point (b)(i) to (iii) above to one of their members. The coordinator retains sole responsibility for compliance with the obligations under the Agreement.

The beneficiaries must have **internal arrangements** regarding their operation and co-ordination, to ensure that the action is implemented properly.

If required by the granting authority (see Data Sheet, Point 1), these arrangements must be set out in a written **consortium agreement** between the beneficiaries, covering for instance:

¹² For the definition, see Article 187(2) EU Financial Regulation 2018/1046: “Where several entities satisfy the criteria for being awarded a grant and together form one entity, that entity may be treated as the **sole beneficiary**, including where it is specifically established for the purpose of implementing the action financed by the grant.”

- the internal organisation of the consortium
- the management of access to the Portal
- different distribution keys for the payments and financial responsibilities in case of recoveries (if any)
- additional rules on rights and obligations related to background and results (see Article 16)
- settlement of internal disputes
- liability, indemnification and confidentiality arrangements between the beneficiaries.

The internal arrangements must not contain any provision contrary to this Agreement.

ARTICLE 8 — AFFILIATED ENTITIES

Not applicable

ARTICLE 9 — OTHER PARTICIPANTS INVOLVED IN THE ACTION

9.1 Associated partners

Not applicable

9.2 Third parties giving in-kind contributions to the action

Other third parties may give in-kind contributions to the action (i.e. personnel, equipment, other goods, works and services, etc. which are free-of-charge), if necessary for the implementation.

Third parties giving in-kind contributions do not implement any action tasks. They may not charge costs or contributions to the action and the costs for the in-kind contributions are not eligible.

The third parties and their in-kind contributions should be set out in Annex 1.

9.3 Subcontractors

Subcontractors may participate in the action, if necessary for the implementation.

Subcontractors must implement their action tasks in accordance with Article 11. The costs for the subcontracted tasks (invoiced price from the subcontractor) are eligible and may be charged by the beneficiaries, under the conditions set out in Article 6. The costs will be included in Annex 2 as part of the beneficiaries' costs.

The beneficiaries must ensure that their contractual obligations under Articles 11 (proper implementation), 12 (conflict of interest), 13 (confidentiality and security), 14 (ethics), 17.2 (visibility), 18 (specific rules for carrying out action), 19 (information) and 20 (record-keeping) also apply to the subcontractors.

The beneficiaries must ensure that the bodies mentioned in Article 25 (e.g. granting authority, OLAF, Court of Auditors (ECA), etc.) can exercise their rights also towards the subcontractors.

9.4 Recipients of financial support to third parties

If the action includes providing financial support to third parties (e.g. grants, prizes or similar forms of support), the beneficiaries must ensure that their contractual obligations under Articles 12 (conflict of interest), 13 (confidentiality and security), 14 (ethics), 17.2 (visibility), 18 (specific rules for carrying out action), 19 (information) and 20 (record-keeping) also apply to the third parties receiving the support (recipients).

The beneficiaries must also ensure that the bodies mentioned in Article 25 (e.g. granting authority, OLAF, Court of Auditors (ECA), etc.) can exercise their rights also towards the recipients.

ARTICLE 10 — PARTICIPANTS WITH SPECIAL STATUS

10.1 Non-EU participants

Participants which are established in a non-EU country (if any) undertake to comply with their obligations under the Agreement and:

- to respect general principles (including fundamental rights, values and ethical principles, environmental and labour standards, rules on classified information, intellectual property rights, visibility of funding and protection of personal data)
- for the submission of certificates under Article 24: to use qualified external auditors which are independent and comply with comparable standards as those set out in EU Directive 2006/43/EC¹³
- for the controls under Article 25: to allow for checks, reviews, audits and investigations (including on-the-spot checks, visits and inspections) by the bodies mentioned in that Article (e.g. granting authority, OLAF, Court of Auditors (ECA), etc.).

Special rules on dispute settlement apply (see Data Sheet, Point 5).

10.2 Participants which are international organisations

Participants which are international organisations (IOs; if any) undertake to comply with their obligations under the Agreement and:

- to respect general principles (including fundamental rights, values and ethical principles, environmental and labour standards, rules on classified information, intellectual property rights, visibility of funding and protection of personal data)
- for the submission of certificates under Article 24: to use either independent public officers or external auditors which comply with comparable standards as those set out in EU Directive 2006/43/EC
- for the controls under Article 25: to allow for the checks, reviews, audits and investigations by the bodies mentioned in that Article, taking into account the specific agreements concluded by them and the EU (if any).

¹³ Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts or similar national regulations (OJ L 157, 9.6.2006, p. 87).

For such participants, nothing in the Agreement will be interpreted as a waiver of their privileges or immunities, as accorded by their constituent documents or international law.

Special rules on applicable law and dispute settlement apply (see Article 43 and Data Sheet, Point 5).

10.3 Pillar-assessed participants

Pillar-assessed participants (if any) may rely on their own systems, rules and procedures, in so far as they have been positively assessed and do not call into question the decision awarding the grant or breach the principle of equal treatment of applicants or beneficiaries.

‘Pillar-assessment’ means a review by the European Commission on the systems, rules and procedures which participants use for managing EU grants (in particular internal control system, accounting system, external audits, financing of third parties, rules on recovery and exclusion, information on recipients and protection of personal data; see Article 154 EU Financial Regulation 2018/1046).

Participants with a positive pillar assessment may rely on their own systems, rules and procedures, in particular for:

- record-keeping (Article 20): may be done in accordance with internal standards, rules and procedures
- currency conversion for financial statements (Article 21): may be done in accordance with usual accounting practices
- guarantees (Article 23): for public law bodies, prefinancing guarantees are not needed
- certificates (Article 24):
 - certificates on the financial statements (CFS): may be provided by their regular internal or external auditors and in accordance with their internal financial regulations and procedures
 - certificates on usual accounting practices (CoMUC): are not needed if those practices are covered by an ex-ante assessment

and use the following specific rules, for:

- recoveries (Article 22): in case of financial support to third parties, there will be no recovery if the participant has done everything possible to retrieve the undue amounts from the third party receiving the support (including legal proceedings) and non-recovery is not due to an error or negligence on its part
- checks, reviews, audits and investigations by the EU (Article 25): will be conducted taking into account the rules and procedures specifically agreed between them and the framework agreement (if any)
- impact evaluation (Article 26): will be conducted in accordance with the participant’s internal rules and procedures and the framework agreement (if any)
- grant agreement suspension (Article 31): certain costs incurred during grant suspension are eligible (notably, minimum costs necessary for a possible resumption of the action and costs

relating to contracts which were entered into before the pre-information letter was received and which could not reasonably be suspended, reallocated or terminated on legal grounds)

- grant agreement termination (Article 32): the final grant amount and final payment will be calculated taking into account also costs relating to contracts due for execution only after termination takes effect, if the contract was entered into before the pre-information letter was received and could not reasonably be terminated on legal grounds
- liability for damages (Article 33.2): the granting authority must be compensated for damage it sustains as a result of the implementation of the action or because the action was not implemented in full compliance with the Agreement only if the damage is due to an infringement of the participant's internal rules and procedures or due to a violation of third parties' rights by the participant or one of its employees or individual for whom the employees are responsible.

Participants whose pillar assessment covers procurement and granting procedures may also do purchases, subcontracting and financial support to third parties (Article 6.2) in accordance with their internal rules and procedures for purchases, subcontracting and financial support.

Participants whose pillar assessment covers data protection rules may rely on their internal standards, rules and procedures for data protection (Article 15).

The participants may however not rely on provisions which would breach the principle of equal treatment of applicants or beneficiaries or call into question the decision awarding the grant, such as in particular:

- eligibility (Article 6)
- consortium roles and set-up (Articles 7-9)
- security and ethics (Articles 13, 14)
- IPR (including background and results, access rights and rights of use), communication, dissemination and visibility (Articles 16 and 17)
- information obligation (Article 19)
- payment, reporting and amendments (Articles 21, 22 and 39)
- rejections, reductions, suspensions and terminations (Articles 27, 28, 29-32)

If the pillar assessment was subject to remedial measures, reliance on the internal systems, rules and procedures is subject to compliance with those remedial measures.

Participants whose assessment has not yet been updated to cover (the new rules on) data protection may rely on their internal systems, rules and procedures, provided that they ensure that personal data is:

- processed lawfully, fairly and in a transparent manner in relation to the data subject
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed and
- processed in a manner that ensures appropriate security of the personal data.

Participants must inform the coordinator without delay of any changes to the systems, rules and procedures that were part of the pillar assessment. The coordinator must immediately inform the granting authority.

Pillar-assessed participants that have also concluded a framework agreement with the EU, may moreover — under the same conditions as those above (i.e. not call into question the decision awarding the grant or breach the principle of equal treatment of applicants or beneficiaries) — rely on the provisions set out in that framework agreement.

SECTION 2 RULES FOR CARRYING OUT THE ACTION

ARTICLE 11 — PROPER IMPLEMENTATION OF THE ACTION

11.1 Obligation to properly implement the action

The beneficiaries must implement the action as described in Annex 1 and in compliance with the provisions of the Agreement, the call conditions and all legal obligations under applicable EU, international and national law.

11.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28).

Such breaches may also lead to other measures described in Chapter 5.

ARTICLE 12 — CONFLICT OF INTERESTS

12.1 Conflict of interests

The beneficiaries must take all measures to prevent any situation where the impartial and objective implementation of the Agreement could be compromised for reasons involving family, emotional life, political or national affinity, economic interest or any other direct or indirect interest (‘conflict of interests’).

They must formally notify the granting authority without delay of any situation constituting or likely to lead to a conflict of interests and immediately take all the necessary steps to rectify this situation.

The granting authority may verify that the measures taken are appropriate and may require additional measures to be taken by a specified deadline.

12.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28) and the grant or the beneficiary may be terminated (see Article 32).

Such breaches may also lead to other measures described in Chapter 5.

ARTICLE 13 — CONFIDENTIALITY AND SECURITY

13.1 Sensitive information

The parties must keep confidential any data, documents or other material (in any form) that is identified as sensitive in writing ('sensitive information') — during the implementation of the action and for at least until the time-limit set out in the Data Sheet (see Point 6).

If a beneficiary requests, the granting authority may agree to keep such information confidential for a longer period.

Unless otherwise agreed between the parties, they may use sensitive information only to implement the Agreement.

The beneficiaries may disclose sensitive information to their personnel or other participants involved in the action only if they:

- (a) need to know it in order to implement the Agreement and
- (b) are bound by an obligation of confidentiality.

The granting authority may disclose sensitive information to its staff and to other EU institutions and bodies.

It may moreover disclose sensitive information to third parties, if:

- (a) this is necessary to implement the Agreement or safeguard the EU financial interests and
- (b) the recipients of the information are bound by an obligation of confidentiality.

The confidentiality obligations no longer apply if:

- (a) the disclosing party agrees to release the other party
- (b) the information becomes publicly available, without breaching any confidentiality obligation
- (c) the disclosure of the sensitive information is required by EU, international or national law.

Specific confidentiality rules (if any) are set out in Annex 5.

13.2 Classified information

The parties must handle classified information in accordance with the applicable EU, international or national law on classified information (in particular, Decision 2015/444¹⁴ and its implementing rules).

Deliverables which contain classified information must be submitted according to special procedures agreed with the granting authority.

Action tasks involving classified information may be subcontracted only after explicit approval (in writing) from the granting authority.

Classified information may not be disclosed to any third party (including participants involved in the action implementation) without prior explicit written approval from the granting authority.

Specific security rules (if any) are set out in Annex 5.

13.3 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28).

Such breaches may also lead to other measures described in Chapter 5.

ARTICLE 14 — ETHICS AND VALUES

14.1 Ethics

The action must be carried out in line with the highest ethical standards and the applicable EU, international and national law on ethical principles.

Specific ethics rules (if any) are set out in Annex 5.

14.2 Values

The beneficiaries must commit to and ensure the respect of basic EU values (such as respect for human dignity, freedom, democracy, equality, the rule of law and human rights, including the rights of minorities).

Specific rules on values (if any) are set out in Annex 5.

14.3 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28).

Such breaches may also lead to other measures described in Chapter 5.

ARTICLE 15 — DATA PROTECTION

15.1 Data processing by the granting authority

¹⁴ Commission Decision 2015/444/EC, Euratom of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

Any personal data under the Agreement will be processed under the responsibility of the data controller of the granting authority in accordance with and for the purposes set out in the Portal Privacy Statement.

For grants where the granting authority is the European Commission, an EU regulatory or executive agency, joint undertaking or other EU body, the processing will be subject to Regulation 2018/1725¹⁵.

15.2 Data processing by the beneficiaries

The beneficiaries must process personal data under the Agreement in compliance with the applicable EU, international and national law on data protection (in particular, Regulation 2016/679¹⁶).

They must ensure that personal data is:

- processed lawfully, fairly and in a transparent manner in relation to the data subjects
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed and
- processed in a manner that ensures appropriate security of the data.

The beneficiaries may grant their personnel access to personal data only if it is strictly necessary for implementing, managing and monitoring the Agreement. The beneficiaries must ensure that the personnel is under a confidentiality obligation.

The beneficiaries must inform the persons whose data are transferred to the granting authority and provide them with the Portal Privacy Statement.

15.3 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28).

Such breaches may also lead to other measures described in Chapter 5.

ARTICLE 16 — INTELLECTUAL PROPERTY RIGHTS (IPR) — BACKGROUND AND RESULTS — ACCESS RIGHTS AND RIGHTS OF USE

¹⁵ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

¹⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('GDPR') (OJ L 119, 4.5.2016, p. 1).

16.1 Background and access rights to background

The beneficiaries must give each other and the other participants access to the background identified as needed for implementing the action, subject to any specific rules in Annex 5.

‘Background’ means any data, know-how or information — whatever its form or nature (tangible or intangible), including any rights such as intellectual property rights — that is:

- (a) held by the beneficiaries before they acceded to the Agreement and
- (b) needed to implement the action or exploit the results.

If background is subject to rights of a third party, the beneficiary concerned must ensure that it is able to comply with its obligations under the Agreement.

16.2 Ownership of results

The granting authority does not obtain ownership of the results produced under the action.

‘Results’ means any tangible or intangible effect of the action, such as data, know-how or information, whatever its form or nature, whether or not it can be protected, as well as any rights attached to it, including intellectual property rights.

16.3 Rights of use of the granting authority on materials, documents and information received for policy, information, communication, dissemination and publicity purposes

The granting authority has the right to use non-sensitive information relating to the action and materials and documents received from the beneficiaries (notably summaries for publication, deliverables, as well as any other material, such as pictures or audio-visual material, in paper or electronic form) for policy, information, communication, dissemination and publicity purposes — during the action or afterwards.

The right to use the beneficiaries’ materials, documents and information is granted in the form of a royalty-free, non-exclusive and irrevocable licence, which includes the following rights:

- (a) **use for its own purposes** (in particular, making them available to persons working for the granting authority or any other EU service (including institutions, bodies, offices, agencies, etc.) or EU Member State institution or body; copying or reproducing them in whole or in part, in unlimited numbers; and communication through press information services)
- (b) **distribution to the public** (in particular, publication as hard copies and in electronic or digital format, publication on the internet, as a downloadable or non-downloadable file, broadcasting by any channel, public display or presentation, communicating through press information services, or inclusion in widely accessible databases or indexes)
- (c) **editing or redrafting** (including shortening, summarising, inserting other elements (e.g. meta-data, legends, other graphic, visual, audio or text elements), extracting parts (e.g. audio or video files), dividing into parts, use in a compilation)
- (d) **translation**
- (e) **storage** in paper, electronic or other form

- (f) **archiving**, in line with applicable document-management rules
- (g) the right to authorise **third parties** to act on its behalf or sub-license to third parties the modes of use set out in Points (b), (c), (d) and (f), if needed for the information, communication and publicity activity of the granting authority
- (h) **processing**, analysing, aggregating the materials, documents and information received and **producing derivative works**.

The rights of use are granted for the whole duration of the industrial or intellectual property rights concerned.

If materials or documents are subject to moral rights or third party rights (including intellectual property rights or rights of natural persons on their image and voice), the beneficiaries must ensure that they comply with their obligations under this Agreement (in particular, by obtaining the necessary licences and authorisations from the rights holders concerned).

Where applicable, the granting authority will insert the following information:

“© – [year] – [name of the copyright owner]. All rights reserved. Licensed to the [name of granting authority] under conditions.”

16.4 Specific rules on IPR, results and background

Specific rules regarding intellectual property rights, results and background (if any) are set out in Annex 5.

16.5 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28).

Such a breach may also lead to other measures described in Chapter 5.

ARTICLE 17 — COMMUNICATION, DISSEMINATION AND VISIBILITY

17.1 Communication — Dissemination — Promoting the action

Unless otherwise agreed with the granting authority, the beneficiaries must promote the action and its results by providing targeted information to multiple audiences (including the media and the public), in accordance with Annex 1 and in a strategic, coherent and effective manner.

Before engaging in a communication or dissemination activity expected to have a major media impact, the beneficiaries must inform the granting authority.

17.2 Visibility — European flag and funding statement

Unless otherwise agreed with the granting authority, communication activities of the beneficiaries related to the action (including media relations, conferences, seminars, information material, such as brochures, leaflets, posters, presentations, etc., in electronic form, via traditional or social media, etc.), dissemination activities and any infrastructure, equipment, vehicles, supplies or major result funded

by the grant must acknowledge EU support and display the European flag (emblem) and funding statement (translated into local languages, where appropriate):



Funded by the
European Union



Co-funded by the
European Union



Funded by the
European Union



Co-funded by the
European Union

The emblem must remain distinct and separate and cannot be modified by adding other visual marks, brands or text.

Apart from the emblem, no other visual identity or logo may be used to highlight the EU support.

When displayed in association with other logos (e.g. of beneficiaries or sponsors), the emblem must be displayed at least as prominently and visibly as the other logos.

For the purposes of their obligations under this Article, the beneficiaries may use the emblem without first obtaining approval from the granting authority. This does not, however, give them the right to exclusive use. Moreover, they may not appropriate the emblem or any similar trademark or logo, either by registration or by any other means.

17.3 Quality of information — Disclaimer

Any communication or dissemination activity related to the action must use factually accurate information.

Moreover, it must indicate the following disclaimer (translated into local languages where appropriate):

“Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them.”

17.4 Specific communication, dissemination and visibility rules

Specific communication, dissemination and visibility rules (if any) are set out in Annex 5.

17.5 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28).

Such breaches may also lead to other measures described in Chapter 5.

ARTICLE 18 — SPECIFIC RULES FOR CARRYING OUT THE ACTION

18.1 Specific rules for carrying out the action

Specific rules for implementing the action (if any) are set out in Annex 5.

18.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28).

Such a breach may also lead to other measures described in Chapter 5.

SECTION 3 GRANT ADMINISTRATION

ARTICLE 19 — GENERAL INFORMATION OBLIGATIONS

19.1 Information requests

The beneficiaries must provide — during the action or afterwards and in accordance with Article 7 — any information requested in order to verify eligibility of the costs or contributions declared, proper implementation of the action and compliance with the other obligations under the Agreement.

The information provided must be accurate, precise and complete and in the format requested, including electronic format.

19.2 Participant Register data updates

The beneficiaries must keep — at all times, during the action or afterwards — their information stored in the Portal Participant Register up to date, in particular, their name, address, legal representatives, legal form and organisation type.

19.3 Information about events and circumstances which impact the action

The beneficiaries must immediately inform the granting authority (and the other beneficiaries) of any of the following:

- (a) **events** which are likely to affect or delay the implementation of the action or affect the EU's financial interests, in particular:
 - (i) changes in their legal, financial, technical, organisational or ownership situation (including changes linked to one of the exclusion grounds listed in the declaration of honour signed before grant signature)

(ii) linked action information: not applicable

(b) **circumstances** affecting:

(i) the decision to award the grant or

(ii) compliance with requirements under the Agreement.

19.4 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28).

Such breaches may also lead to other measures described in Chapter 5.

ARTICLE 20 — RECORD-KEEPING

20.1 Keeping records and supporting documents

The beneficiaries must — at least until the time-limit set out in the Data Sheet (see Point 6) — keep records and other supporting documents to prove the proper implementation of the action in line with the accepted standards in the respective field (if any).

In addition, the beneficiaries must — for the same period — keep the following to justify the amounts declared:

- (a) for actual costs: adequate records and supporting documents to prove the costs declared (such as contracts, subcontracts, invoices and accounting records); in addition, the beneficiaries' usual accounting and internal control procedures must enable direct reconciliation between the amounts declared, the amounts recorded in their accounts and the amounts stated in the supporting documents
- (b) for flat-rate costs and contributions (if any): adequate records and supporting documents to prove the eligibility of the costs or contributions to which the flat-rate is applied
- (c) for the following simplified costs and contributions: the beneficiaries do not need to keep specific records on the actual costs incurred, but must keep:
 - (i) for unit costs and contributions (if any): adequate records and supporting documents to prove the number of units declared
 - (ii) for lump sum costs and contributions (if any): adequate records and supporting documents to prove proper implementation of the work as described in Annex 1
 - (iii) for financing not linked to costs (if any): adequate records and supporting documents to prove the achievement of the results or the fulfilment of the conditions as described in Annex 1
- (d) for unit, flat-rate and lump sum costs and contributions according to usual cost accounting practices (if any): the beneficiaries must keep any adequate records and supporting documents to prove that their cost accounting practices have been applied in a consistent manner, based on

objective criteria, regardless of the source of funding, and that they comply with the eligibility conditions set out in Articles 6.1 and 6.2.

Moreover, the following is needed for specific budget categories:

- (e) for personnel costs: time worked for the beneficiary under the action must be supported by declarations signed monthly by the person and their supervisor, unless another reliable time-record system is in place; the granting authority may accept alternative evidence supporting the time worked for the action declared, if it considers that it offers an adequate level of assurance
- (f) additional record-keeping rules: not applicable

The records and supporting documents must be made available upon request (see Article 19) or in the context of checks, reviews, audits or investigations (see Article 25).

If there are on-going checks, reviews, audits, investigations, litigation or other pursuits of claims under the Agreement (including the extension of findings; see Article 25), the beneficiaries must keep these records and other supporting documentation until the end of these procedures.

The beneficiaries must keep the original documents. Digital and digitalised documents are considered originals if they are authorised by the applicable national law. The granting authority may accept non-original documents if they offer a comparable level of assurance.

20.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, costs or contributions insufficiently substantiated will be ineligible (see Article 6) and will be rejected (see Article 27), and the grant may be reduced (see Article 28).

Such breaches may also lead to other measures described in Chapter 5.

ARTICLE 21 — REPORTING

21.1 Continuous reporting

The beneficiaries must continuously report on the progress of the action (e.g. **deliverables, milestones, outputs/outcomes, critical risks, indicators**, etc; if any), in the Portal Continuous Reporting tool and in accordance with the timing and conditions it sets out (as agreed with the granting authority).

Standardised deliverables (e.g. progress reports not linked to payments, reports on cumulative expenditure, special reports, etc; if any) must be submitted using the templates published on the Portal.

21.2 Periodic reporting: Technical reports and financial statements

In addition, the beneficiaries must provide reports to request payments, in accordance with the schedule and modalities set out in the Data Sheet (see Point 4.2):

- for additional prefinancings (if any): an **additional prefinancing report**
- for interim payments (if any) and the final payment: a **periodic report**.

The prefinancing and periodic reports include a technical and financial part.

The technical part includes an overview of the action implementation. It must be prepared using the template available in the Portal Periodic Reporting tool.

The financial part of the additional prefinancing report includes a statement on the use of the previous prefinancing payment.

The financial part of the periodic report includes:

- the financial statements (individual and consolidated; for all beneficiaries/affiliated entities)
- the explanation on the use of resources (or detailed cost reporting table, if required)
- the certificates on the financial statements (CFS) (if required; see Article 24.2 and Data Sheet, Point 4.3).

The **financial statements** must detail the eligible costs and contributions for each budget category and, for the final payment, also the revenues for the action (see Articles 6 and 22).

All eligible costs and contributions incurred should be declared, even if they exceed the amounts indicated in the estimated budget (see Annex 2). Amounts that are not declared in the individual financial statements will not be taken into account by the granting authority.

By signing the financial statements (directly in the Portal Periodic Reporting tool), the beneficiaries confirm that:

- the information provided is complete, reliable and true
- the costs and contributions declared are eligible (see Article 6)
- the costs and contributions can be substantiated by adequate records and supporting documents (see Article 20) that will be produced upon request (see Article 19) or in the context of checks, reviews, audits and investigations (see Article 25)
- for the final periodic report: all the revenues have been declared (if required; see Article 22).

Beneficiaries will have to submit also the financial statements of their affiliated entities (if any). In case of recoveries (see Article 22), beneficiaries will be held responsible also for the financial statements of their affiliated entities.

21.3 Currency for financial statements and conversion into euros

The financial statements must be drafted in euro.

Beneficiaries with general accounts established in a currency other than the euro must convert the costs recorded in their accounts into euro, at the average of the daily exchange rates published in the C series of the *Official Journal of the European Union* (ECB website), calculated over the corresponding reporting period.

If no daily euro exchange rate is published in the *Official Journal* for the currency in question, they must be converted at the average of the monthly accounting exchange rates published on the European Commission website (InforEuro), calculated over the corresponding reporting period.

Beneficiaries with general accounts in euro must convert costs incurred in another currency into euro according to their usual accounting practices.

21.4 Reporting language

The reporting must be in the language of the Agreement, unless otherwise agreed with the granting authority (see Data Sheet, Point 4.2).

21.5 Consequences of non-compliance

If a report submitted does not comply with this Article, the granting authority may suspend the payment deadline (see Article 29) and apply other measures described in Chapter 5.

If the coordinator breaches its reporting obligations, the granting authority may terminate the grant or the coordinator's participation (see Article 32) or apply other measures described in Chapter 5.

ARTICLE 22 — PAYMENTS AND RECOVERIES — CALCULATION OF AMOUNTS DUE

22.1 Payments and payment arrangements

Payments will be made in accordance with the schedule and modalities set out in the Data Sheet (see Point 4.2).

They will be made in euro to the bank account indicated by the coordinator (see Data Sheet, Point 4.2) and must be distributed without unjustified delay (restrictions may apply to distribution of the initial prefinancing payment; see Data Sheet, Point 4.2).

Payments to this bank account will discharge the granting authority from its payment obligation.

The cost of payment transfers will be borne as follows:

- the granting authority bears the cost of transfers charged by its bank
- the beneficiary bears the cost of transfers charged by its bank
- the party causing a repetition of a transfer bears all costs of the repeated transfer.

Payments by the granting authority will be considered to have been carried out on the date when they are debited to its account.

22.2 Recoveries

Recoveries will be made, if — at beneficiary termination, final payment or afterwards — it turns out that the granting authority has paid too much and needs to recover the amounts undue.

The general liability regime for recoveries (first-line liability) is as follows: At final payment, the coordinator will be fully liable for recoveries, even if it has not been the final recipient of the undue amounts. At beneficiary termination or after final payment, recoveries will be made directly against the beneficiaries concerned.

Beneficiaries will be fully liable for repaying the debts of their affiliated entities.

In case of enforced recoveries (see Article 22.4):

- the beneficiaries will be jointly and severally liable for repaying debts of another beneficiary under the Agreement (including late-payment interest), if required by the granting authority (see Data Sheet, Point 4.4)
- affiliated entities will be held liable for repaying debts of their beneficiaries under the Agreement (including late-payment interest), if required by the granting authority (see Data Sheet, Point 4.4).

22.3 Amounts due

22.3.1 Prefinancing payments

The aim of the prefinancing is to provide the beneficiaries with a float.

It remains the property of the EU until the final payment.

For **initial prefinancings** (if any), the amount due, schedule and modalities are set out in the Data Sheet (see Point 4.2).

For **additional prefinancings** (if any), the amount due, schedule and modalities are also set out in the Data Sheet (see Point 4.2). However, if the statement on the use of the previous prefinancing payment shows that less than 70% was used, the amount set out in the Data Sheet will be reduced by the difference between the 70% threshold and the amount used.

Prefinancing payments (or parts of them) may be offset (without the beneficiaries' consent) against amounts owed by a beneficiary to the granting authority — up to the amount due to that beneficiary.

For grants where the granting authority is the European Commission or an EU executive agency, offsetting may also be done against amounts owed to other Commission services or executive agencies.

Payments will not be made if the payment deadline or payments are suspended (see Articles 29 and 30).

22.3.2 Amount due at beneficiary termination — Recovery

In case of beneficiary termination, the granting authority will determine the provisional amount due for the beneficiary concerned. Payments (if any) will be made with the next interim or final payment.

The **amount due** will be calculated in the following step:

Step 1 — Calculation of the total accepted EU contribution

Step 1 — Calculation of the total accepted EU contribution

The granting authority will first calculate the 'accepted EU contribution' for the beneficiary for all reporting periods, by calculating the 'maximum EU contribution to costs' (applying the funding rate to the accepted costs of the beneficiary), taking into account requests for a lower contribution to costs and CFS threshold cappings (if any; see Article 24.5) and adding the contributions (accepted unit, flat-rate or lump sum contributions and financing not linked to costs, if any).

After that, the granting authority will take into account grant reductions (if any). The resulting amount is the ‘total accepted EU contribution’ for the beneficiary.

The **balance** is then calculated by deducting the payments received (if any; see report on the distribution of payments in Article 32), from the total accepted EU contribution:

$$\begin{aligned} & \{ \text{total accepted EU contribution for the beneficiary} \\ & \text{minus} \\ & \{ \text{prefinancing and interim payments received (if any)} \} \}. \end{aligned}$$

If the balance is **positive**, the amount will be included in the next interim or final payment to the consortium.

If the balance is **negative**, it will be **recovered** in accordance with the following procedure:

The granting authority will send a **pre-information letter** to the beneficiary concerned:

- formally notifying the intention to recover, the amount due, the amount to be recovered and the reasons why and
- requesting observations within 30 days of receiving notification.

If no observations are submitted (or the granting authority decides to pursue recovery despite the observations it has received), it will confirm the amount to be recovered and ask this amount to be paid to the coordinator (**confirmation letter**).

The amounts will later on also be taken into account for the next interim or final payment.

22.3.3 Interim payments

Interim payments reimburse the eligible costs and contributions claimed for the implementation of the action during the reporting periods (if any).

Interim payments (if any) will be made in accordance with the schedule and modalities set out the Data Sheet (see Point 4.2).

Payment is subject to the approval of the periodic report. Its approval does not imply recognition of compliance, authenticity, completeness or correctness of its content.

The **interim payment** will be calculated by the granting authority in the following steps:

Step 1 — Calculation of the total accepted EU contribution

Step 2 — Limit to the interim payment ceiling

Step 1 — Calculation of the total accepted EU contribution

The granting authority will calculate the ‘accepted EU contribution’ for the action for the reporting period, by first calculating the ‘maximum EU contribution to costs’ (applying the funding rate to the accepted costs of each beneficiary), taking into account requests for a lower contribution to costs, and CFS threshold cappings (if any; see Article 24.5) and adding the contributions (accepted unit, flat-rate or lump sum contributions and financing not linked to costs, if any).

After that, the granting authority will take into account grant reductions from beneficiary termination (if any). The resulting amount is the ‘total accepted EU contribution’.

Step 2 — Limit to the interim payment ceiling

The resulting amount is then capped to ensure that the total amount of prefinancing and interim payments (if any) does not exceed the interim payment ceiling set out in the Data Sheet (see Point 4.2).

Interim payments (or parts of them) may be offset (without the beneficiaries’ consent) against amounts owed by a beneficiary to the granting authority — up to the amount due to that beneficiary.

For grants where the granting authority is the European Commission or an EU executive agency, offsetting may also be done against amounts owed to other Commission services or executive agencies.

Payments will not be made if the payment deadline or payments are suspended (see Articles 29 and 30).

22.3.4 Final payment — Final grant amount — Revenues and Profit — Recovery

The final payment (payment of the balance) reimburses the remaining part of the eligible costs and contributions claimed for the implementation of the action (if any).

The final payment will be made in accordance with the schedule and modalities set out in the Data Sheet (see Point 4.2).

Payment is subject to the approval of the final periodic report. Its approval does not imply recognition of compliance, authenticity, completeness or correctness of its content.

The **final grant amount for the action** will be calculated in the following steps:

Step 1 — Calculation of the total accepted EU contribution

Step 2 — Limit to the maximum grant amount

Step 3 — Reduction due to the no-profit rule

Step 1 — Calculation of the total accepted EU contribution

The granting authority will first calculate the ‘accepted EU contribution’ for the action for all reporting periods, by calculating the ‘maximum EU contribution to costs’ (applying the funding rate to the total accepted costs of each beneficiary), taking into account requests for a lower contribution to costs, CFS threshold cappings (if any; see Article 24.5) and adding the contributions (accepted unit, flat-rate or lump sum contributions and financing not linked to costs, if any).

After that, the granting authority will take into account grant reductions (if any). The resulting amount is the ‘total accepted EU contribution’.

Step 2 — Limit to the maximum grant amount

If the resulting amount is higher than the maximum grant amount set out in Article 5.2, it will be limited to the latter.

Step 3 — Reduction due to the no-profit rule

If the no-profit rule is provided for in the Data Sheet (see Point 4.2), the grant must not produce a profit (i.e. surplus of the amount obtained following Step 2 plus the action's revenues, over the eligible costs and contributions approved by the granting authority).

'Revenue' is all income generated by the action, during its duration (see Article 4), for beneficiaries that are profit legal entities.

If there is a profit, it will be deducted in proportion to the final rate of reimbursement of the eligible costs approved by the granting authority (as compared to the amount calculated following Steps 1 and 2 minus the contributions).

The **balance** (final payment) is then calculated by deducting the total amount of prefinancing and interim payments already made (if any), from the final grant amount:

$$\left\{ \begin{array}{l} \text{final grant amount} \\ \text{minus} \\ \text{prefinancing and interim payments made (if any)} \end{array} \right\}.$$

If the balance is **positive**, it will be **paid** to the coordinator.

The final payment (or part of it) may be offset (without the beneficiaries' consent) against amounts owed by a beneficiary to the granting authority — up to the amount due to that beneficiary.

For grants where the granting authority is the European Commission or an EU executive agency, offsetting may also be done against amounts owed to other Commission services or executive agencies.

Payments will not be made if the payment deadline or payments are suspended (see Articles 29 and 30).

If the balance is **negative**, it will be **recovered** in accordance with the following procedure:

The granting authority will send a **pre-information letter** to the coordinator:

- formally notifying the intention to recover, the final grant amount, the amount to be recovered and the reasons why
- requesting observations within 30 days of receiving notification.

If no observations are submitted (or the granting authority decides to pursue recovery despite the observations it has received), it will confirm the amount to be recovered (**confirmation letter**), together with a **debit note** with the terms and date for payment.

If payment is not made by the date specified in the debit note, the granting authority will **enforce recovery** in accordance with Article 22.4.

22.3.5 Audit implementation after final payment — Revised final grant amount — Recovery

If — after the final payment (in particular, after checks, reviews, audits or investigations; see

Article 25) — the granting authority rejects costs or contributions (see Article 27) or reduces the grant (see Article 28), it will calculate the **revised final grant amount** for the beneficiary concerned.

The **beneficiary revised final grant amount** will be calculated in the following step:

Step 1 — Calculation of the revised total accepted EU contribution

Step 1 — Calculation of the revised total accepted EU contribution

The granting authority will first calculate the ‘revised accepted EU contribution’ for the beneficiary, by calculating the ‘revised accepted costs’ and ‘revised accepted contributions’.

After that, it will take into account grant reductions (if any). The resulting ‘revised total accepted EU contribution’ is the beneficiary revised final grant amount.

If the revised final grant amount is lower than the beneficiary’s final grant amount (i.e. its share in the final grant amount for the action), it will be **recovered** in accordance with the following procedure:

The **beneficiary final grant amount** (i.e. share in the final grant amount for the action) is calculated as follows:

$$\left\{ \begin{array}{l} \text{\{total accepted EU contribution for the beneficiary} \\ \text{divided by} \\ \text{total accepted EU contribution for the action\}} \\ \text{multiplied by} \\ \text{final grant amount for the action\}}. \end{array} \right.$$

The granting authority will send a **pre-information letter** to the beneficiary concerned:

- formally notifying the intention to recover, the amount to be recovered and the reasons why and
- requesting observations within 30 days of receiving notification.

If no observations are submitted (or the granting authority decides to pursue recovery despite the observations it has received), it will confirm the amount to be recovered (**confirmation letter**), together with a **debit note** with the terms and the date for payment.

Recoveries against affiliated entities (if any) will be handled through their beneficiaries.

If payment is not made by the date specified in the debit note, the granting authority will **enforce recovery** in accordance with Article 22.4.

22.4 Enforced recovery

If payment is not made by the date specified in the debit note, the amount due will be recovered:

- (a) by offsetting the amount — without the coordinator or beneficiary’s consent — against any amounts owed to the coordinator or beneficiary by the granting authority.

In exceptional circumstances, to safeguard the EU financial interests, the amount may be offset before the payment date specified in the debit note.

For grants where the granting authority is the European Commission or an EU executive agency, debts may also be offset against amounts owed by other Commission services or executive agencies.

- (b) by drawing on the financial guarantee(s) (if any)
- (c) by holding other beneficiaries jointly and severally liable (if any; see Data Sheet, Point 4.4)
- (d) by holding affiliated entities jointly and severally liable (if any, see Data Sheet, Point 4.4)
- (e) by taking legal action (see Article 43) or, provided that the granting authority is the European Commission or an EU executive agency, by adopting an enforceable decision under Article 299 of the Treaty on the Functioning of the EU (TFEU) and Article 100(2) of EU Financial Regulation 2018/1046.

The amount to be recovered will be increased by **late-payment interest** at the rate set out in Article 22.5, from the day following the payment date in the debit note, up to and including the date the full payment is received.

Partial payments will be first credited against expenses, charges and late-payment interest and then against the principal.

Bank charges incurred in the recovery process will be borne by the beneficiary, unless Directive 2015/2366¹⁷ applies.

For grants where the granting authority is an EU executive agency, enforced recovery by offsetting or enforceable decision will be done by the services of the European Commission (see also Article 43).

22.5 Consequences of non-compliance

22.5.1 If the granting authority does not pay within the payment deadlines (see above), the beneficiaries are entitled to **late-payment interest** at the rate applied by the European Central Bank (ECB) for its main refinancing operations in euros ('reference rate'), plus the rate specified in the Data Sheet (Point 4.2). The reference rate is the rate in force on the first day of the month in which the payment deadline expires, as published in the C series of the *Official Journal of the European Union*.

If the late-payment interest is lower than or equal to EUR 200, it will be paid to the coordinator only on request submitted within two months of receiving the late payment.

Late-payment interest is not due if all beneficiaries are EU Member States (including regional and local government authorities or other public bodies acting on behalf of a Member State for the purpose of this Agreement).

If payments or the payment deadline are suspended (see Articles 29 and 30), payment will not be considered as late.

¹⁷ Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

Late-payment interest covers the period running from the day following the due date for payment (see above), up to and including the date of payment.

Late-payment interest is not considered for the purposes of calculating the final grant amount.

22.5.2 If the coordinator breaches any of its obligations under this Article, the grant may be reduced (see Article 29) and the grant or the coordinator may be terminated (see Article 32).

Such breaches may also lead to other measures described in Chapter 5.

ARTICLE 23 — GUARANTEES

23.1 Prefinancing guarantee

If required by the granting authority (see Data Sheet, Point 4.2), the beneficiaries must provide (one or more) prefinancing guarantee(s) in accordance with the timing and the amounts set out in the Data Sheet.

The coordinator must submit them to the granting authority in due time before the prefinancing they are linked to.

The guarantees must be drawn up using the template published on the Portal and fulfil the following conditions:

- (a) be provided by a bank or approved financial institution established in the EU or — if requested by the coordinator and accepted by the granting authority — by a third party or a bank or financial institution established outside the EU offering equivalent security
- (b) the guarantor stands as first-call guarantor and does not require the granting authority to first have recourse against the principal debtor (i.e. the beneficiary concerned) and
- (c) remain explicitly in force until the final payment and, if the final payment takes the form of a recovery, until five months after the debit note is notified to a beneficiary.

They will be released within the following month.

23.2 Consequences of non-compliance

If the beneficiaries breach their obligation to provide the prefinancing guarantee, the prefinancing will not be paid.

Such breaches may also lead to other measures described in Chapter 5.

ARTICLE 24 — CERTIFICATES

24.1 Operational verification report (OVR)

Not applicable

24.2 Certificate on the financial statements (CFS)

If required by the granting authority (see Data Sheet, Point 4.3), the beneficiaries must provide

certificates on their financial statements (CFS), in accordance with the schedule, threshold and conditions set out in the Data Sheet.

The coordinator must submit them as part of the periodic report (see Article 21).

The certificates must be drawn up using the template published on the Portal, cover the costs declared on the basis of actual costs and costs according to usual cost accounting practices (if any), and fulfil the following conditions:

- (a) be provided by a qualified approved external auditor which is independent and complies with Directive 2006/43/EC¹⁸ (or for public bodies: by a competent independent public officer)
- (b) the verification must be carried out according to the highest professional standards to ensure that the financial statements comply with the provisions under the Agreement and that the costs declared are eligible.

The certificates will not affect the granting authority's right to carry out its own checks, reviews or audits, nor preclude the European Court of Auditors (ECA), the European Public Prosecutor's Office (EPPO) or the European Anti-Fraud Office (OLAF) from using their prerogatives for audits and investigations under the Agreement (see Article 25).

If the costs (or a part of them) were already audited by the granting authority, these costs do not need to be covered by the certificate and will not be counted for calculating the threshold (if any).

24.3 Certificate on the compliance of usual cost accounting practices (CoMUC)

Beneficiaries which use unit, flat rate or lump sum costs or contributions according to usual costs accounting practices (if any) may submit to the granting authority, for approval, a certificate on the methodology stating that their usual cost accounting practices comply with the eligibility conditions under the Agreement.

The certificate must be drawn up using the template published on the Portal and fulfil the following conditions:

- (a) be provided by a qualified approved external auditor which is independent and complies with Directive 2006/43/EC¹⁹ (or for public bodies: by a competent independent public officer)
- (b) the verification must be carried out according to the highest professional standards to ensure that the methodology for declaring costs according to usual accounting practices complies with the provisions under the Agreement.

If the certificate is approved, amounts declared in line with this methodology will not be challenged subsequently, unless the beneficiary concealed information for the purpose of the approval.

24.4 Systems and process audit (SPA)

Not applicable

¹⁸ Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts or similar national regulations (OJ L 157, 9.6.2006, p. 87).

¹⁹ Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts or similar national regulations (OJ L 157, 9.6.2006, p. 87).

24.5 Consequences of non-compliance

If a beneficiary does not submit a certificate on the financial statements (CFS) or the certificate is rejected, the accepted EU contribution to costs will be capped to reflect the CFS threshold.

If a beneficiary breaches any of its other obligations under this Article, the granting authority may apply the measures described in Chapter 5.

ARTICLE 25 — CHECKS, REVIEWS, AUDITS AND INVESTIGATIONS — EXTENSION OF FINDINGS

25.1 Granting authority checks, reviews and audits

25.1.1 Internal checks

The granting authority may — during the action or afterwards — check the proper implementation of the action and compliance with the obligations under the Agreement, including assessing costs and contributions, deliverables and reports.

25.1.2 Project reviews

The granting authority may carry out reviews on the proper implementation of the action and compliance with the obligations under the Agreement (general project reviews or specific issues reviews).

Such project reviews may be started during the implementation of the action and until the time-limit set out in the Data Sheet (see Point 6). They will be formally notified to the coordinator or beneficiary concerned and will be considered to start on the date of the notification.

If needed, the granting authority may be assisted by independent, outside experts. If it uses outside experts, the coordinator or beneficiary concerned will be informed and have the right to object on grounds of commercial confidentiality or conflict of interest.

The coordinator or beneficiary concerned must cooperate diligently and provide — within the deadline requested — any information and data in addition to deliverables and reports already submitted (including information on the use of resources). The granting authority may request beneficiaries to provide such information to it directly. Sensitive information and documents will be treated in accordance with Article 13.

The coordinator or beneficiary concerned may be requested to participate in meetings, including with the outside experts.

For **on-the-spot visits**, the beneficiary concerned must allow access to sites and premises (including to the outside experts) and must ensure that information requested is readily available.

Information provided must be accurate, precise and complete and in the format requested, including electronic format.

On the basis of the review findings, a **project review report** will be drawn up.

The granting authority will formally notify the project review report to the coordinator or beneficiary concerned, which has 30 days from receiving notification to make observations.

Project reviews (including project review reports) will be in the language of the Agreement.

25.1.3 Audits

The granting authority may carry out audits on the proper implementation of the action and compliance with the obligations under the Agreement.

Such audits may be started during the implementation of the action and until the time-limit set out in the Data Sheet (see Point 6). They will be formally notified to the beneficiary concerned and will be considered to start on the date of the notification.

The granting authority may use its own audit service, delegate audits to a centralised service or use external audit firms. If it uses an external firm, the beneficiary concerned will be informed and have the right to object on grounds of commercial confidentiality or conflict of interest.

The beneficiary concerned must cooperate diligently and provide — within the deadline requested — any information (including complete accounts, individual salary statements or other personal data) to verify compliance with the Agreement. Sensitive information and documents will be treated in accordance with Article 13.

For **on-the-spot** visits, the beneficiary concerned must allow access to sites and premises (including for the external audit firm) and must ensure that information requested is readily available.

Information provided must be accurate, precise and complete and in the format requested, including electronic format.

On the basis of the audit findings, a **draft audit report** will be drawn up.

The auditors will formally notify the draft audit report to the beneficiary concerned, which has 30 days from receiving notification to make observations (contradictory audit procedure).

The **final audit report** will take into account observations by the beneficiary concerned and will be formally notified to them.

Audits (including audit reports) will be in the language of the Agreement.

25.2 European Commission checks, reviews and audits in grants of other granting authorities

Where the granting authority is not the European Commission, the latter has the same rights of checks, reviews and audits as the granting authority.

25.3 Access to records for assessing simplified forms of funding

The beneficiaries must give the European Commission access to their statutory records for the periodic assessment of simplified forms of funding which are used in EU programmes.

25.4 OLAF, EPPO and ECA audits and investigations

The following bodies may also carry out checks, reviews, audits and investigations — during the action or afterwards:

- the European Anti-Fraud Office (OLAF) under Regulations No 883/2013²⁰ and No 2185/96²¹
- the European Public Prosecutor's Office (EPPO) under Regulation 2017/1939
- the European Court of Auditors (ECA) under Article 287 of the Treaty on the Functioning of the EU (TFEU) and Article 257 of EU Financial Regulation 2018/1046.

If requested by these bodies, the beneficiary concerned must provide full, accurate and complete information in the format requested (including complete accounts, individual salary statements or other personal data, including in electronic format) and allow access to sites and premises for on-the-spot visits or inspections — as provided for under these Regulations.

To this end, the beneficiary concerned must keep all relevant information relating to the action, at least until the time-limit set out in the Data Sheet (Point 6) and, in any case, until any ongoing checks, reviews, audits, investigations, litigation or other pursuits of claims have been concluded.

25.5 Consequences of checks, reviews, audits and investigations — Extension of results of reviews, audits or investigations

25.5.1 Consequences of checks, reviews, audits and investigations in this grant

Findings in checks, reviews, audits or investigations carried out in the context of this grant may lead to rejections (see Article 27), grant reduction (see Article 28) or other measures described in Chapter 5.

Rejections or grant reductions after the final payment will lead to a revised final grant amount (see Article 22).

Findings in checks, reviews, audits or investigations during the action implementation may lead to a request for amendment (see Article 39), to change the description of the action set out in Annex 1.

Checks, reviews, audits or investigations that find systemic or recurrent errors, irregularities, fraud or breach of obligations in any EU grant may also lead to consequences in other EU grants awarded under similar conditions ('extension to other grants').

Moreover, findings arising from an OLAF or EPPO investigation may lead to criminal prosecution under national law.

25.5.2 Extension from other grants

Results of checks, reviews, audits or investigations in other grants may be extended to this grant, if:

- (a) the beneficiary concerned is found, in other EU grants awarded under similar conditions, to have committed systemic or recurrent errors, irregularities, fraud or breach of obligations that have a material impact on this grant and

²⁰ Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18/09/2013, p. 1).

²¹ Council Regulation (Euratom, EC) No 2185/1996 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities (OJ L 292, 15/11/1996, p. 2).

- (b) those findings are formally notified to the beneficiary concerned — together with the list of grants affected by the findings — within the time-limit for audits set out in the Data Sheet (see Point 6).

The granting authority will formally notify the beneficiary concerned of the intention to extend the findings and the list of grants affected.

If the extension concerns **rejections of costs or contributions**: the notification will include:

- (a) an invitation to submit observations on the list of grants affected by the findings
- (b) the request to submit revised financial statements for all grants affected
- (c) the correction rate for extrapolation, established on the basis of the systemic or recurrent errors, to calculate the amounts to be rejected, if the beneficiary concerned:
 - (i) considers that the submission of revised financial statements is not possible or practicable or
 - (ii) does not submit revised financial statements.

If the extension concerns **grant reductions**: the notification will include:

- (a) an invitation to submit observations on the list of grants affected by the findings and
- (b) the **correction rate for extrapolation**, established on the basis of the systemic or recurrent errors and the principle of proportionality.

The beneficiary concerned has **60 days** from receiving notification to submit observations, revised financial statements or to propose a duly substantiated **alternative correction method/rate**.

On the basis of this, the granting authority will analyse the impact and decide on the implementation (i.e. start rejection or grant reduction procedures, either on the basis of the revised financial statements or the announced/alternative method/rate or a mix of those; see Articles 27 and 28).

25.6 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, costs or contributions insufficiently substantiated will be ineligible (see Article 6) and will be rejected (see Article 27), and the grant may be reduced (see Article 28).

Such breaches may also lead to other measures described in Chapter 5.

ARTICLE 26 — IMPACT EVALUATIONS

26.1 Impact evaluation

The granting authority may carry out impact evaluations of the action, measured against the objectives and indicators of the EU programme funding the grant.

Such evaluations may be started during implementation of the action and until the time-limit set out

in the Data Sheet (see Point 6). They will be formally notified to the coordinator or beneficiaries and will be considered to start on the date of the notification.

If needed, the granting authority may be assisted by independent outside experts.

The coordinator or beneficiaries must provide any information relevant to evaluate the impact of the action, including information in electronic format.

26.2 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the granting authority may apply the measures described in Chapter 5.

CHAPTER 5 CONSEQUENCES OF NON-COMPLIANCE

SECTION 1 REJECTIONS AND GRANT REDUCTION

ARTICLE 27 — REJECTION OF COSTS AND CONTRIBUTIONS

27.1 Conditions

The granting authority will — at beneficiary termination, interim payment, final payment or afterwards — reject any costs or contributions which are ineligible (see Article 6), in particular following checks, reviews, audits or investigations (see Article 25).

The rejection may also be based on the extension of findings from other grants to this grant (see Article 25).

Ineligible costs or contributions will be rejected.

27.2 Procedure

If the rejection does not lead to a recovery, the granting authority will formally notify the coordinator or beneficiary concerned of the rejection, the amounts and the reasons why. The coordinator or beneficiary concerned may — within 30 days of receiving notification — submit observations if it disagrees with the rejection (payment review procedure).

If the rejection leads to a recovery, the granting authority will follow the contradictory procedure with pre-information letter set out in Article 22.

27.3 Effects

If the granting authority rejects costs or contributions, it will deduct them from the costs or contributions declared and then calculate the amount due (and, if needed, make a recovery; see Article 22).

ARTICLE 28 — GRANT REDUCTION

28.1 Conditions

The granting authority may — at beneficiary termination, final payment or afterwards — reduce the grant for a beneficiary, if:

- (a) the beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed:
 - (i) substantial errors, irregularities or fraud or
 - (ii) serious breach of obligations under this Agreement or during its award (including improper implementation of the action, non-compliance with the call conditions, submission of false information, failure to provide required information, breach of ethics or security rules (if applicable), etc.), or
- (b) the beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed — in other EU grants awarded to it under similar conditions — systemic or recurrent errors, irregularities, fraud or serious breach of obligations that have a material impact on this grant (see Article 25).

The amount of the reduction will be calculated for each beneficiary concerned and proportionate to the seriousness and the duration of the errors, irregularities or fraud or breach of obligations, by applying an individual reduction rate to their accepted EU contribution.

28.2 Procedure

If the grant reduction does not lead to a recovery, the granting authority will formally notify the coordinator or beneficiary concerned of the reduction, the amount to be reduced and the reasons why. The coordinator or beneficiary concerned may — within 30 days of receiving notification — submit observations if it disagrees with the reduction (payment review procedure).

If the grant reduction leads to a recovery, the granting authority will follow the contradictory procedure with pre-information letter set out in Article 22.

28.3 Effects

If the granting authority reduces the grant, it will deduct the reduction and then calculate the amount due (and, if needed, make a recovery; see Article 22).

SECTION 2 SUSPENSION AND TERMINATION

ARTICLE 29 — PAYMENT DEADLINE SUSPENSION

29.1 Conditions

The granting authority may — at any moment — suspend the payment deadline if a payment cannot be processed because:

- (a) the required report (see Article 21) has not been submitted or is not complete or additional information is needed
- (b) there are doubts about the amount to be paid (e.g. ongoing audit extension procedure, queries

about eligibility, need for a grant reduction, etc.) and additional checks, reviews, audits or investigations are necessary, or

- (c) there are other issues affecting the EU financial interests.

29.2 Procedure

The granting authority will formally notify the coordinator of the suspension and the reasons why.

The suspension will **take effect** the day the notification is sent.

If the conditions for suspending the payment deadline are no longer met, the suspension will be **lifted** — and the remaining time to pay (see Data Sheet, Point 4.2) will resume.

If the suspension exceeds two months, the coordinator may request the granting authority to confirm if the suspension will continue.

If the payment deadline has been suspended due to the non-compliance of the report and the revised report is not submitted (or was submitted but is also rejected), the granting authority may also terminate the grant or the participation of the coordinator (see Article 32).

ARTICLE 30 — PAYMENT SUSPENSION

30.1 Conditions

The granting authority may — at any moment — suspend payments, in whole or in part for one or more beneficiaries, if:

- (a) a beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed or is suspected of having committed:
 - (i) substantial errors, irregularities or fraud or
 - (ii) serious breach of obligations under this Agreement or during its award (including improper implementation of the action, non-compliance with the call conditions, submission of false information, failure to provide required information, breach of ethics or security rules (if applicable), etc.), or
- (b) a beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed — in other EU grants awarded to it under similar conditions — systemic or recurrent errors, irregularities, fraud or serious breach of obligations that have a material impact on this grant.

If payments are suspended for one or more beneficiaries, the granting authority will make partial payment(s) for the part(s) not suspended. If suspension concerns the final payment, the payment (or recovery) of the remaining amount after suspension is lifted will be considered to be the payment that closes the action.

30.2 Procedure

Before suspending payments, the granting authority will send a **pre-information letter** to the beneficiary concerned:

- formally notifying the intention to suspend payments and the reasons why and
- requesting observations within 30 days of receiving notification.

If the granting authority does not receive observations or decides to pursue the procedure despite the observations it has received, it will confirm the suspension (**confirmation letter**). Otherwise, it will formally notify that the procedure is discontinued.

At the end of the suspension procedure, the granting authority will also inform the coordinator.

The suspension will **take effect** the day after the confirmation notification is sent.

If the conditions for resuming payments are met, the suspension will be **lifted**. The granting authority will formally notify the beneficiary concerned (and the coordinator) and set the suspension end date.

During the suspension, no prefinancing will be paid to the beneficiaries concerned. For interim payments, the periodic reports for all reporting periods except the last one (see Article 21) must not contain any financial statements from the beneficiary concerned (or its affiliated entities). The coordinator must include them in the next periodic report after the suspension is lifted or — if suspension is not lifted before the end of the action — in the last periodic report.

ARTICLE 31 — GRANT AGREEMENT SUSPENSION

31.1 Consortium-requested GA suspension

31.1.1 Conditions and procedure

The beneficiaries may request the suspension of the grant or any part of it, if exceptional circumstances — in particular *force majeure* (see Article 35) — make implementation impossible or excessively difficult.

The coordinator must submit a request for **amendment** (see Article 39), with:

- the reasons why
- the date the suspension takes effect; this date may be before the date of the submission of the amendment request and
- the expected date of resumption.

The suspension will **take effect** on the day specified in the amendment.

Once circumstances allow for implementation to resume, the coordinator must immediately request another **amendment** of the Agreement to set the suspension end date, the resumption date (one day after suspension end date), extend the duration and make other changes necessary to adapt the action to the new situation (see Article 39) — unless the grant has been terminated (see Article 32). The suspension will be **lifted** with effect from the suspension end date set out in the amendment. This date may be before the date of the submission of the amendment request.

During the suspension, no prefinancing will be paid. Costs incurred or contributions for activities implemented during grant suspension are not eligible (see Article 6.3).

31.2 EU-initiated GA suspension

31.2.1 Conditions

The granting authority may suspend the grant or any part of it, if:

- (a) a beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed or is suspected of having committed:
 - (i) substantial errors, irregularities or fraud or
 - (ii) serious breach of obligations under this Agreement or during its award (including improper implementation of the action, non-compliance with the call conditions, submission of false information, failure to provide required information, breach of ethics or security rules (if applicable), etc.), or
- (b) a beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed — in other EU grants awarded to it under similar conditions — systemic or recurrent errors, irregularities, fraud or serious breach of obligations that have a material impact on this grant
- (c) other:
 - (i) linked action issues: not applicable
 - (ii) additional GA suspension grounds: not applicable.

31.2.2 Procedure

Before suspending the grant, the granting authority will send a **pre-information letter** to the coordinator:

- formally notifying the intention to suspend the grant and the reasons why and
- requesting observations within 30 days of receiving notification.

If the granting authority does not receive observations or decides to pursue the procedure despite the observations it has received, it will confirm the suspension (**confirmation letter**). Otherwise, it will formally notify that the procedure is discontinued.

The suspension will **take effect** the day after the confirmation notification is sent (or on a later date specified in the notification).

Once the conditions for resuming implementation of the action are met, the granting authority will formally notify the coordinator a **lifting of suspension letter**, in which it will set the suspension end date and invite the coordinator to request an amendment of the Agreement to set the resumption date (one day after suspension end date), extend the duration and make other changes necessary to adapt the action to the new situation (see Article 39) — unless the grant has been terminated (see

Article 32). The suspension will be **lifted** with effect from the suspension end date set out in the lifting of suspension letter. This date may be before the date on which the letter is sent.

During the suspension, no prefinancing will be paid. Costs incurred or contributions for activities implemented during suspension are not eligible (see Article 6.3).

The beneficiaries may not claim damages due to suspension by the granting authority (see Article 33).

Grant suspension does not affect the granting authority's right to terminate the grant or a beneficiary (see Article 32) or reduce the grant (see Article 28).

ARTICLE 32 — GRANT AGREEMENT OR BENEFICIARY TERMINATION

32.1 Consortium-requested GA termination

32.1.1 Conditions and procedure

The beneficiaries may request the termination of the grant.

The coordinator must submit a request for **amendment** (see Article 39), with:

- the reasons why
- the date the consortium ends work on the action ('end of work date') and
- the date the termination takes effect ('termination date'); this date must be after the date of the submission of the amendment request.

The termination will **take effect** on the termination date specified in the amendment.

If no reasons are given or if the granting authority considers the reasons do not justify termination, it may consider the grant terminated improperly.

32.1.2 Effects

The coordinator must — within 60 days from when termination takes effect — submit a **periodic report** (for the open reporting period until termination).

The granting authority will calculate the final grant amount and final payment on the basis of the report submitted and taking into account the costs incurred and contributions for activities implemented before the end of work date (see Article 22). Costs relating to contracts due for execution only after the end of work are not eligible.

If the granting authority does not receive the report within the deadline, only costs and contributions which are included in an approved periodic report will be taken into account (no costs/contributions if no periodic report was ever approved).

Improper termination may lead to a grant reduction (see Article 28).

After termination, the beneficiaries' obligations (in particular Articles 13 (confidentiality and security), 16 (IPR), 17 (communication, dissemination and visibility), 21 (reporting), 25 (checks, reviews, audits and investigations), 26 (impact evaluation), 27 (rejections), 28 (grant reduction) and 42 (assignment of claims)) continue to apply.

32.2 Consortium-requested beneficiary termination

32.2.1 Conditions and procedure

The coordinator may request the termination of the participation of one or more beneficiaries, on request of the beneficiary concerned or on behalf of the other beneficiaries.

The coordinator must submit a request for **amendment** (see Article 39), with:

- the reasons why
- the opinion of the beneficiary concerned (or proof that this opinion has been requested in writing)
- the date the beneficiary ends work on the action ('end of work date')
- the date the termination takes effect ('termination date'); this date must be after the date of the submission of the amendment request.

If the termination concerns the coordinator and is done without its agreement, the amendment request must be submitted by another beneficiary (acting on behalf of the consortium).

The termination will **take effect** on the termination date specified in the amendment.

If no information is given or if the granting authority considers that the reasons do not justify termination, it may consider the beneficiary to have been terminated improperly.

32.2.2 Effects

The coordinator must — within 60 days from when termination takes effect — submit:

- (i) a **report on the distribution of payments** to the beneficiary concerned
- (ii) a **termination report** from the beneficiary concerned, for the open reporting period until termination, containing an overview of the progress of the work, the financial statement, the explanation on the use of resources, and, if applicable, the certificate on the financial statement (CFS; see Articles 21 and 24.2 and Data Sheet, Point 4.3)
- (iii) a second **request for amendment** (see Article 39) with other amendments needed (e.g. reallocation of the tasks and the estimated budget of the terminated beneficiary; addition of a new beneficiary to replace the terminated beneficiary; change of coordinator, etc.).

The granting authority will calculate the amount due to the beneficiary on the basis of the report submitted and taking into account the costs incurred and contributions for activities implemented before the end of work date (see Article 22). Costs relating to contracts due for execution only after the end of work are not eligible.

The information in the termination report must also be included in the periodic report for the next reporting period (see Article 21).

If the granting authority does not receive the termination report within the deadline, only costs and contributions which are included in an approved periodic report will be taken into account (no costs/contributions if no periodic report was ever approved).

If the granting authority does not receive the report on the distribution of payments within the deadline, it will consider that:

- the coordinator did not distribute any payment to the beneficiary concerned and that
- the beneficiary concerned must not repay any amount to the coordinator.

If the second request for amendment is accepted by the granting authority, the Agreement is **amended** to introduce the necessary changes (see Article 39).

If the second request for amendment is rejected by the granting authority (because it calls into question the decision awarding the grant or breaches the principle of equal treatment of applicants), the grant may be terminated (see Article 32).

Improper termination may lead to a reduction of the grant (see Article 31) or grant termination (see Article 32).

After termination, the concerned beneficiary's obligations (in particular Articles 13 (confidentiality and security), 16 (IPR), 17 (communication, dissemination and visibility), 21 (reporting), 25 (checks, reviews, audits and investigations), 26 (impact evaluation), 27 (rejections), 28 (grant reduction) and 42 (assignment of claims)) continue to apply.

32.3 EU-initiated GA or beneficiary termination

32.3.1 Conditions

The granting authority may terminate the grant or the participation of one or more beneficiaries, if:

- (a) one or more beneficiaries do not accede to the Agreement (see Article 40)
- (b) a change to the action or the legal, financial, technical, organisational or ownership situation of a beneficiary is likely to substantially affect the implementation of the action or calls into question the decision to award the grant (including changes linked to one of the exclusion grounds listed in the declaration of honour)
- (c) following termination of one or more beneficiaries, the necessary changes to the Agreement (and their impact on the action) would call into question the decision awarding the grant or breach the principle of equal treatment of applicants
- (d) implementation of the action has become impossible or the changes necessary for its continuation would call into question the decision awarding the grant or breach the principle of equal treatment of applicants
- (e) a beneficiary (or person with unlimited liability for its debts) is subject to bankruptcy proceedings or similar (including insolvency, winding-up, administration by a liquidator or court, arrangement with creditors, suspension of business activities, etc.)
- (f) a beneficiary (or person with unlimited liability for its debts) is in breach of social security or tax obligations
- (g) a beneficiary (or person having powers of representation, decision-making or control, or person

essential for the award/implementation of the grant) has been found guilty of grave professional misconduct

- (h) a beneficiary (or person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed fraud, corruption, or is involved in a criminal organisation, money laundering, terrorism-related crimes (including terrorism financing), child labour or human trafficking
- (i) a beneficiary (or person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) was created under a different jurisdiction with the intent to circumvent fiscal, social or other legal obligations in the country of origin (or created another entity with this purpose)
- (j) a beneficiary (or person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed:
 - (i) substantial errors, irregularities or fraud or
 - (ii) serious breach of obligations under this Agreement or during its award (including improper implementation of the action, non-compliance with the call conditions, submission of false information, failure to provide required information, breach of ethics or security rules (if applicable), etc.)
- (k) a beneficiary (or person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed — in other EU grants awarded to it under similar conditions — systemic or recurrent errors, irregularities, fraud or serious breach of obligations that have a material impact on this grant (extension of findings from other grants to this grant; see Article 25)
- (l) despite a specific request by the granting authority, a beneficiary does not request — through the coordinator — an amendment to the Agreement to end the participation of one of its affiliated entities or associated partners that is in one of the situations under points (d), (f), (e), (g), (h), (i) or (j) and to reallocate its tasks, or
- (m) other:
 - (i) linked action issues: not applicable
 - (ii) additional GA termination grounds: not applicable.

32.3.2 Procedure

Before terminating the grant or participation of one or more beneficiaries, the granting authority will send a **pre-information letter** to the coordinator or beneficiary concerned:

- formally notifying the intention to terminate and the reasons why and
- requesting observations within 30 days of receiving notification.

If the granting authority does not receive observations or decides to pursue the procedure despite the observations it has received, it will confirm the termination and the date it will take effect (**confirmation letter**). Otherwise, it will formally notify that the procedure is discontinued.

For beneficiary terminations, the granting authority will — at the end of the procedure — also inform the coordinator.

The termination will **take effect** the day after the confirmation notification is sent (or on a later date specified in the notification; ‘termination date’).

32.3.3 Effects

(a) for **GA termination**:

The coordinator must — within 60 days from when termination takes effect — submit a **periodic report** (for the last open reporting period until termination).

The granting authority will calculate the final grant amount and final payment on the basis of the report submitted and taking into account the costs incurred and contributions for activities implemented before termination takes effect (see Article 22). Costs relating to contracts due for execution only after termination are not eligible.

If the grant is terminated for breach of the obligation to submit reports, the coordinator may not submit any report after termination.

If the granting authority does not receive the report within the deadline, only costs and contributions which are included in an approved periodic report will be taken into account (no costs/contributions if no periodic report was ever approved).

Termination does not affect the granting authority’s right to reduce the grant (see Article 28) or to impose administrative sanctions (see Article 34).

The beneficiaries may not claim damages due to termination by the granting authority (see Article 33).

After termination, the beneficiaries’ obligations (in particular Articles 13 (confidentiality and security), 16 (IPR), 17 (communication, dissemination and visibility), 21 (reporting), 25 (checks, reviews, audits and investigations), 26 (impact evaluation), 27 (rejections), 28 (grant reduction) and 42 (assignment of claims)) continue to apply.

(b) for **beneficiary termination**:

The coordinator must — within 60 days from when termination takes effect — submit:

- (i) a **report on the distribution of payments** to the beneficiary concerned
- (ii) a **termination report** from the beneficiary concerned, for the open reporting period until termination, containing an overview of the progress of the work, the financial statement, the explanation on the use of resources, and, if applicable, the certificate on the financial statement (CFS; see Articles 21 and 24.2 and Data Sheet, Point 4.3)
- (iii) a **request for amendment** (see Article 39) with any amendments needed (e.g. reallocation of the tasks and the estimated budget of the terminated beneficiary; addition of a new beneficiary to replace the terminated beneficiary; change of coordinator, etc.).

The granting authority will calculate the amount due to the beneficiary on the basis of the

report submitted and taking into account the costs incurred and contributions for activities implemented before termination takes effect (see Article 22). Costs relating to contracts due for execution only after termination are not eligible.

The information in the termination report must also be included in the periodic report for the next reporting period (see Article 21).

If the granting authority does not receive the termination report within the deadline, only costs and contributions included in an approved periodic report will be taken into account (no costs/contributions if no periodic report was ever approved).

If the granting authority does not receive the report on the distribution of payments within the deadline, it will consider that:

- the coordinator did not distribute any payment to the beneficiary concerned and that
- the beneficiary concerned must not repay any amount to the coordinator.

If the request for amendment is accepted by the granting authority, the Agreement is **amended** to introduce the necessary changes (see Article 39).

If the request for amendment is rejected by the granting authority (because it calls into question the decision awarding the grant or breaches the principle of equal treatment of applicants), the grant may be terminated (see Article 32).

After termination, the concerned beneficiary's obligations (in particular Articles 13 (confidentiality and security), 16 (IPR), 17 (communication, dissemination and visibility), 21 (reporting), 25 (checks, reviews, audits and investigations), 26 (impact evaluation), 27 (rejections), 28 (grant reduction) and 42 (assignment of claims)) continue to apply.

SECTION 3 OTHER CONSEQUENCES: DAMAGES AND ADMINISTRATIVE SANCTIONS

ARTICLE 33 — DAMAGES

33.1 Liability of the granting authority

The granting authority cannot be held liable for any damage caused to the beneficiaries or to third parties as a consequence of the implementation of the Agreement, including for gross negligence.

The granting authority cannot be held liable for any damage caused by any of the beneficiaries or other participants involved in the action, as a consequence of the implementation of the Agreement.

33.2 Liability of the beneficiaries

The beneficiaries must compensate the granting authority for any damage it sustains as a result of the implementation of the action or because the action was not implemented in full compliance with the Agreement, provided that it was caused by gross negligence or wilful act.

The liability does not extend to indirect or consequential losses or similar damage (such as loss of

profit, loss of revenue or loss of contracts), provided such damage was not caused by wilful act or by a breach of confidentiality.

ARTICLE 34 — ADMINISTRATIVE SANCTIONS AND OTHER MEASURES

Nothing in this Agreement may be construed as preventing the adoption of administrative sanctions (i.e. exclusion from EU award procedures and/or financial penalties) or other public law measures, in addition or as an alternative to the contractual measures provided under this Agreement (see, for instance, Articles 135 to 145 EU Financial Regulation 2018/1046 and Articles 4 and 7 of Regulation 2988/95²²).

SECTION 4 FORCE MAJEURE

ARTICLE 35 — FORCE MAJEURE

A party prevented by force majeure from fulfilling its obligations under the Agreement cannot be considered in breach of them.

‘Force majeure’ means any situation or event that:

- prevents either party from fulfilling their obligations under the Agreement,
- was unforeseeable, exceptional situation and beyond the parties’ control,
- was not due to error or negligence on their part (or on the part of other participants involved in the action), and
- proves to be inevitable in spite of exercising all due diligence.

Any situation constituting force majeure must be formally notified to the other party without delay, stating the nature, likely duration and foreseeable effects.

The parties must immediately take all the necessary steps to limit any damage due to force majeure and do their best to resume implementation of the action as soon as possible.

CHAPTER 6 FINAL PROVISIONS

ARTICLE 36 — COMMUNICATION BETWEEN THE PARTIES

36.1 Forms and means of communication — Electronic management

EU grants are managed fully electronically through the EU Funding & Tenders Portal (‘Portal’).

All communications must be made electronically through the Portal, in accordance with the Portal Terms and Conditions and using the forms and templates provided there (except if explicitly instructed otherwise by the granting authority).

²² Council Regulation (EC, Euratom) No 2988/95 of 18 December 1995 on the protection of the European Communities financial interests (OJ L 312, 23.12.1995, p. 1).

Communications must be made in writing and clearly identify the grant agreement (project number and acronym).

Communications must be made by persons authorised according to the Portal Terms and Conditions. For naming the authorised persons, each beneficiary must have designated — before the signature of this Agreement — a ‘legal entity appointed representative (LEAR)’. The role and tasks of the LEAR are stipulated in their appointment letter (see Portal Terms and Conditions).

If the electronic exchange system is temporarily unavailable, instructions will be given on the Portal.

36.2 Date of communication

The sending date for communications made through the Portal will be the date and time of sending, as indicated by the time logs.

The receiving date for communications made through the Portal will be the date and time the communication is accessed, as indicated by the time logs. Formal notifications that have not been accessed within 10 days after sending, will be considered to have been accessed (see Portal Terms and Conditions).

If a communication is exceptionally made on paper (by e-mail or postal service), general principles apply (i.e. date of sending/receipt). Formal notifications by registered post with proof of delivery will be considered to have been received either on the delivery date registered by the postal service or the deadline for collection at the post office.

If the electronic exchange system is temporarily unavailable, the sending party cannot be considered in breach of its obligation to send a communication within a specified deadline.

36.3 Addresses for communication

The Portal can be accessed via the Europa website.

The address for paper communications to the granting authority (if exceptionally allowed) is the official mailing address indicated on its website.

For beneficiaries, it is the legal address specified in the Portal Participant Register.

ARTICLE 37 — INTERPRETATION OF THE AGREEMENT

The provisions in the Data Sheet take precedence over the rest of the Terms and Conditions of the Agreement.

Annex 5 takes precedence over the Terms and Conditions; the Terms and Conditions take precedence over the Annexes other than Annex 5.

Annex 2 takes precedence over Annex 1.

ARTICLE 38 — CALCULATION OF PERIODS AND DEADLINES

In accordance with Regulation No 1182/71²³, periods expressed in days, months or years are calculated from the moment the triggering event occurs.

The day during which that event occurs is not considered as falling within the period.

‘Days’ means calendar days, not working days.

ARTICLE 39 — AMENDMENTS

39.1 Conditions

The Agreement may be amended, unless the amendment entails changes to the Agreement which would call into question the decision awarding the grant or breach the principle of equal treatment of applicants.

Amendments may be requested by any of the parties.

39.2 Procedure

The party requesting an amendment must submit a request for amendment signed directly in the Portal Amendment tool.

The coordinator submits and receives requests for amendment on behalf of the beneficiaries (see Annex 3). If a change of coordinator is requested without its agreement, the submission must be done by another beneficiary (acting on behalf of the other beneficiaries).

The request for amendment must include:

- the reasons why
- the appropriate supporting documents and
- for a change of coordinator without its agreement: the opinion of the coordinator (or proof that this opinion has been requested in writing).

The granting authority may request additional information.

If the party receiving the request agrees, it must sign the amendment in the tool within 45 days of receiving notification (or any additional information the granting authority has requested). If it does not agree, it must formally notify its disagreement within the same deadline. The deadline may be extended, if necessary for the assessment of the request. If no notification is received within the deadline, the request is considered to have been rejected.

An amendment **enters into force** on the day of the signature of the receiving party.

An amendment **takes effect** on the date of entry into force or other date specified in the amendment.

ARTICLE 40 — ACCESSION AND ADDITION OF NEW BENEFICIARIES

²³ Regulation (EEC, Euratom) No 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time-limits (OJ L 124, 8/6/1971, p. 1).

40.1 Accession of the beneficiaries mentioned in the Preamble

The beneficiaries which are not coordinator must accede to the grant by signing the accession form (see Annex 3) directly in the Portal Grant Preparation tool, within 30 days after the entry into force of the Agreement (see Article 44).

They will assume the rights and obligations under the Agreement with effect from the date of its entry into force (see Article 44).

If a beneficiary does not accede to the grant within the above deadline, the coordinator must — within 30 days — request an amendment (see Article 39) to terminate the beneficiary and make any changes necessary to ensure proper implementation of the action. This does not affect the granting authority's right to terminate the grant (see Article 32).

40.2 Addition of new beneficiaries

In justified cases, the beneficiaries may request the addition of a new beneficiary.

For this purpose, the coordinator must submit a request for amendment in accordance with Article 39. It must include an accession form (see Annex 3) signed by the new beneficiary directly in the Portal Amendment tool.

New beneficiaries will assume the rights and obligations under the Agreement with effect from the date of their accession specified in the accession form (see Annex 3).

Additions are also possible in mono-beneficiary grants.

ARTICLE 41 — TRANSFER OF THE AGREEMENT

In justified cases, the beneficiary of a mono-beneficiary grant may request the transfer of the grant to a new beneficiary, provided that this would not call into question the decision awarding the grant or breach the principle of equal treatment of applicants.

The beneficiary must submit a request for **amendment** (see Article 39), with

- the reasons why
- the accession form (see Annex 3) signed by the new beneficiary directly in the Portal Amendment tool and
- additional supporting documents (if required by the granting authority).

The new beneficiary will assume the rights and obligations under the Agreement with effect from the date of accession specified in the accession form (see Annex 3).

ARTICLE 42 — ASSIGNMENTS OF CLAIMS FOR PAYMENT AGAINST THE GRANTING AUTHORITY

The beneficiaries may not assign any of their claims for payment against the granting authority to any third party, except if expressly approved in writing by the granting authority on the basis of a reasoned, written request by the coordinator (on behalf of the beneficiary concerned).

If the granting authority has not accepted the assignment or if the terms of it are not observed, the assignment will have no effect on it.

In no circumstances will an assignment release the beneficiaries from their obligations towards the granting authority.

ARTICLE 43 — APPLICABLE LAW AND SETTLEMENT OF DISPUTES

43.1 Applicable law

The Agreement is governed by the applicable EU law, supplemented if necessary by the law of Belgium.

Special rules may apply for beneficiaries which are international organisations (if any; see Data Sheet, Point 5).

43.2 Dispute settlement

If a dispute concerns the interpretation, application or validity of the Agreement, the parties must bring action before the EU General Court — or, on appeal, the EU Court of Justice — under Article 272 of the Treaty on the Functioning of the EU (TFEU).

For non-EU beneficiaries (if any), such disputes must be brought before the courts of Brussels, Belgium — unless an international agreement provides for the enforceability of EU court judgements.

For beneficiaries with arbitration as special dispute settlement forum (if any; see Data Sheet, Point 5), the dispute will — in the absence of an amicable settlement — be settled in accordance with the Rules for Arbitration published on the Portal.

If a dispute concerns administrative sanctions, offsetting or an enforceable decision under Article 299 TFEU (see Articles 22 and 34), the beneficiaries must bring action before the General Court — or, on appeal, the Court of Justice — under Article 263 TFEU.

For grants where the granting authority is an EU executive agency (see Preamble), actions against offsetting and enforceable decisions must be brought against the European Commission (not against the granting authority; see also Article 22).

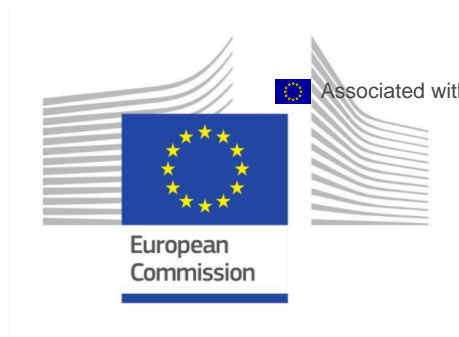
ARTICLE 44 — ENTRY INTO FORCE

The Agreement will enter into force on the day of signature by the granting authority or the coordinator, depending on which is later.

SIGNATURES

For the coordinator

For the granting authority



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	
<i>Grant Preparation (General Information screen) — Enter the info.</i>	
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	3
List of participants	3
List of work packages	4
Staff effort	8
List of deliverables	9
List of milestones (outputs/outcomes)	16
List of critical risks	16

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

LIST OF WORK PACKAGES

Work packages						
<i>Grant Preparation (Work Packages screen) — Enter the info.</i>						
Work Package No	Work Package name	Lead Beneficiary	Effort (Person-Months)	Start Month	End Month	Deliverables
WP1	Design	2 - PAHLDATA	17.00	1	4	D1.1 – First Project Report D1.2 – (Output: Framework v1.0)
WP2	Market Test	1 - INEM	23.00	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)
WP3	Conception & Application	2 - PAHLDATA	23.00	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	17.00	23	24	D4.1 – Final Project Report, including: - Final Framework - Final Training - Final Process D4.2 – Framework Operation Process

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
						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
<p>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.</p> <p>2 - Market Research (Application Questionnaires: Application of questionnaires and interviews to the Intervening Entities.</p> <p>3 - Framework Design V1.0: Security Controls Framework Design (v1.0): Security Dimensions and Dimensional Controls.</p> <p>4 - Market Self-Assessment: Market Self-Assessment (I)</p>

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
<ul style="list-style-type: none"> - 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
<p>5 - Taxonomy Threats and Attack Methods: Analyse, obtain or develop a taxonomy of threats/attack methods.</p> <p>6 - Scenarios Threats and Attack Methods: Build and describe the main attack method scenarios / scenarios (use attack method modelling techniques and Use Cases).</p> <p>7 - Interviews - Focus Groups - Use Cases: Perform the Interviews: Focus Group (Uses Cases and requirements specification).</p> <p>8 - Design Framework V.2.0: Design of the Security Controls Framework (v2.0): baselines by security dimension and control maturity levels.</p> <p>9 - Training & Awareness: Training, Awareness and Training Program in the implementation and operation of the Framework (v1.0).</p> <p>10 - Framework Support Application: Análise e desenho da Ferramenta de suporte (v1.0)</p> <p>11 – Website: Website design and release of version 1.0</p> <p>12 - Market Self-Assessment: Market Self Assessment (II)</p>

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

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

- 19 - Delivering and make availability of the HISC4All Tool: Availability of the Framework Support Application and Implementation Process (HISC4ALL Tool - Website v 3.0)
 20 - 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
 21 -Implementation Plan: Preparation of the plan to follow up on the Framework design project carried out
 22 - Final Report + Translations: Final report

STAFF EFFORT

Staff effort per participant					
<i>Grant Preparation (Work packages - Effort screen) — Enter the info.</i>					
Participant	WP1	WP2	WP3	WP4	Total Person-Months
1 - INEM	7.00	11.00	11.00	7.00	36.00
2 - PAHLDATA	10.00	12.00	12.00	10.00	44.00
Total Person-Months	17.00	23.00	23.00	17.00	80.00

LIST OF DELIVERABLES

Deliverables						
<i>Grant Preparation (Deliverables screen) — Enter the info.</i>						
<i>The labels used mean:</i>						
<i>Public — fully open (⚠ automatically posted online)</i>						
<i>Sensitive — limited under the conditions of the Grant Agreement</i>						
<i>EU classified — RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision 2015/444</i>						
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
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 in the implementation and operation of the Framework (v2.0)	WP3	1 - INEM	R — Document, report	SEN - Sensitive	16

Deliverables						
<i>Grant Preparation (Deliverables screen) — Enter the info.</i>						
<i>The labels used mean:</i>						
<i>Public — fully open (⚠ automatically posted online)</i>						
<i>Sensitive — limited under the conditions of the Grant Agreement</i>						
<i>EU classified —RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision 2015/444</i>						
Deliverable No	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month)
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	1 - INEM	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	2 - PAHLDATA	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	1 - INEM	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 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	1. INEM
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	2. PAHLDATA
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	1. INEM
Deliverable Name	Webinar		
Type	OTHER	Dissemination Level	PU - Public
Due Date (month)	24	Work Package No	WP4

Description
Webinar.

LIST OF MILESTONES

Milestones					
<i>Grant Preparation (Milestones screen) — Enter the info.</i>					
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			
<i>Grant Preparation (Critical Risks screen) — Enter the info.</i>			
Risk number	Description	Work Package No(s)	Proposed Mitigation Measures
1	Unavailability of stakeholders in continuous monitoring of the project	WP4, WP2, WP1, WP3	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - Define the work schedule in a timely manner, based on the project planning;

Critical risks & risk management strategy			
<i>Grant Preparation (Critical Risks screen) — Enter the info.</i>			
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



Digital Europe Programme (DIGITAL)

Description of the action (DoA)

Part B

Version 2.0
09 December 2022





TABLE OF CONTENTS

1. RELEVANCE	3
1.1 Objectives and activities.....	3
1.2 Contribution to long-term policy objectives, policies and strategies — Synergies	9
1.3 Digital technology supply chain	13
2. IMPLEMENTATION	13
2.1 Maturity.....	14
2.2 Implementation plan and efficient use of resources.....	14
2.3 Capacity to carry out the proposed work	24
3. IMPACT	33
3.1 Expected outcomes and deliverables — Dissemination and communication	33
3.2 Competitiveness and benefits for society	35
4. WORK PLAN, TIMING AND SUBCONTRACTING	37
4.1 Work plan	37
4.2 Timetable.....	40
4.3 Subcontracting.....	41
5. ANNEXES	43
5.1 Project Outline	43
5.2 Presentation of the Figures presented in the Formulaire	49
5.3 Detailed Budget	63



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:

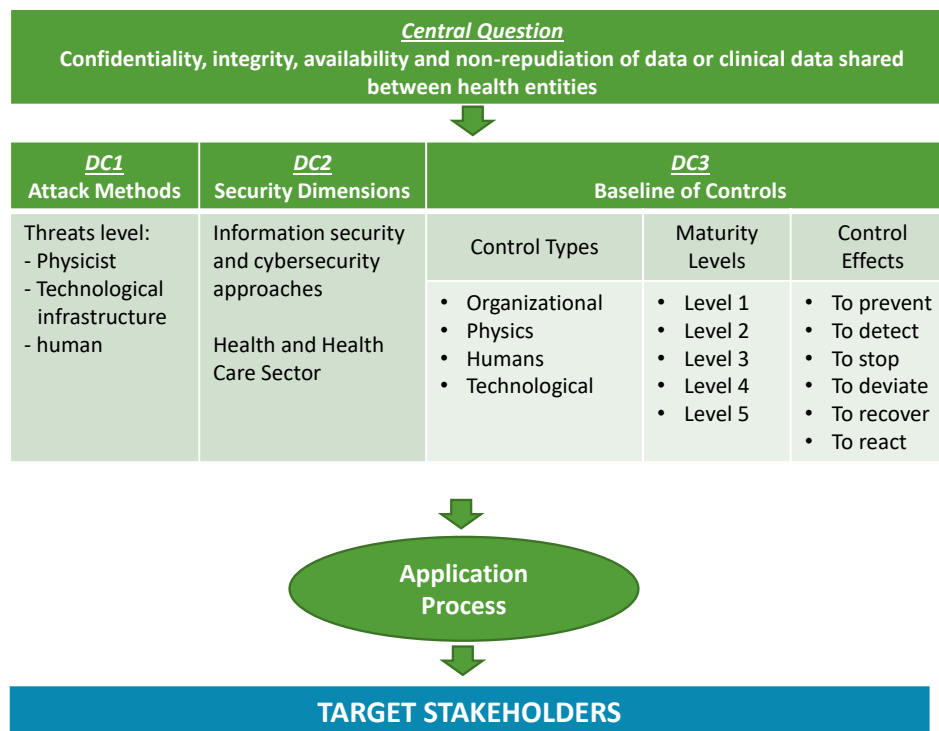


Figure 1 – Framework Configuration

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 (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:

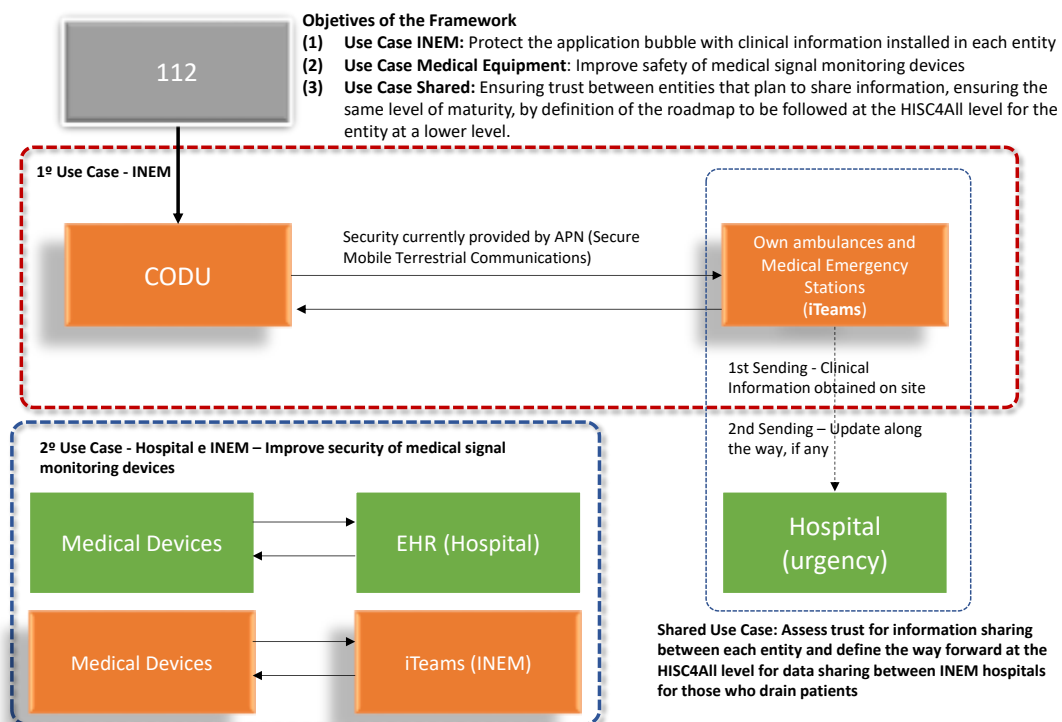


Figure 2 – Use Cases: Project Vision

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.

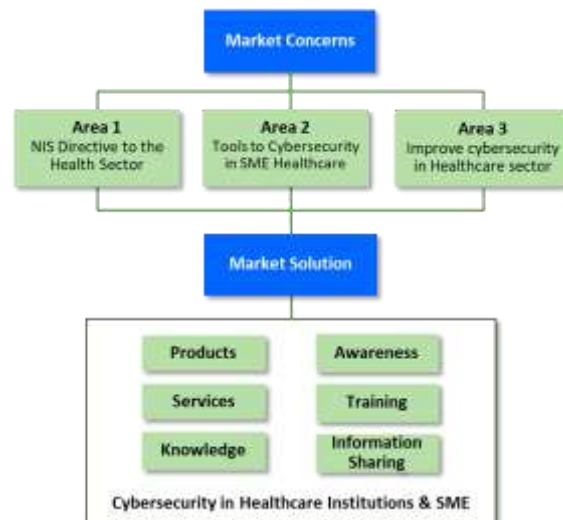


Figure 2 – Use Cases: Project Vision

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

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 service and a private SME specialized in the health sector and healthcare institutions.

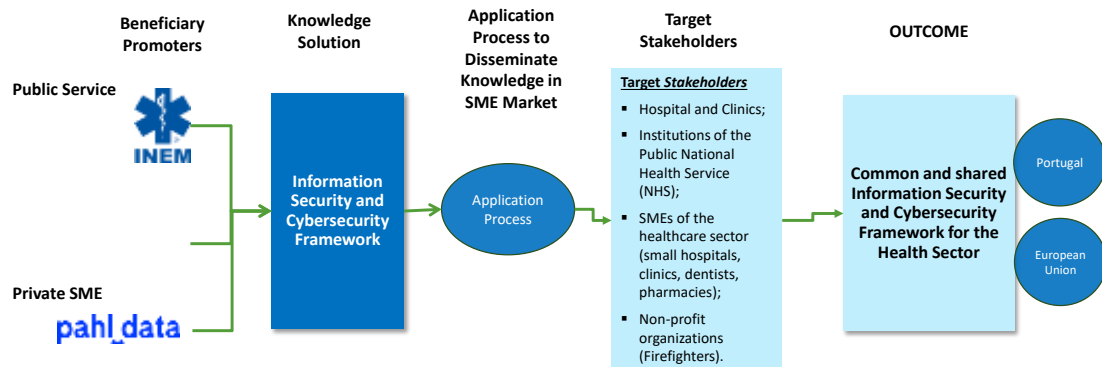


Figure 3 – Introduction of the Framework in the Market

Activities of the Project

Project HISC4ALL will be developed in 4 phases and in 18 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. Design of the Security Controls Framework (v2.0): baselines by security dimension and control maturity levels.

Activity 9. Training, Awareness and Training Program in the implementation and operation of the Framework (v1.0).

Activity 10. Framework Support Application

Activity 11. Website

Activity 12. Market Self-Assessment (II)



Phase III. CONCEPTION & APPLICATION

Activity 13. Design of the framework application process.

Activity 14. Application of the framework to health entities (Action Research – a single cycle)

Activity 15. Collection of lessons learned.

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

Activity 17. HISC4ALL update

Activity 18. Market Validation + Website

PHASE IV. DISSEMINATION

Activity 19. Availability of the HISC4All Tool

Activity 20. Communication & Dissemination Plan + Website

Activity 21. Implementation Plan

Activity 22. 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-run 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.

How the project is based in sound needs analysis in line with European and national level

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.

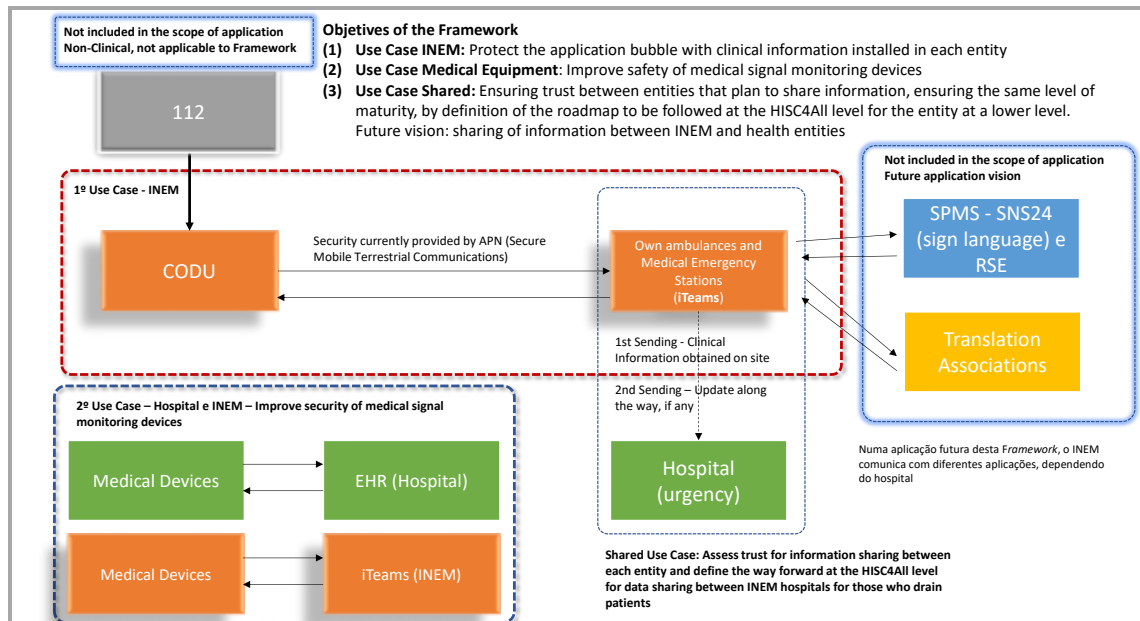


Figure 4 – Use Cases: Project Vision

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 (1^o 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)	<ul style="list-style-type: none"> - National / international standards and references. - Elements for application of questionnaires and interviews. 	<ul style="list-style-type: none"> - Delay in applying questionnaires and conducting interviews (Low Risk). 	<i>SegInfo and Cyber controls framework</i> * (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)	<ul style="list-style-type: none"> - 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 	<ul style="list-style-type: none"> - 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 (2^o 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 (<i>proof of concept: one baseline per dimension of the framework</i>)	- Availability of Entities /Organizations to apply the framework (Low Risk).	<i>Framework Application Process (v1.0).</i> <i>Security Controls Framework (v3.0).</i> <i>Partial report of project no. 3.</i> <i>(Outputs: Framework v3.0 and Application Process)</i>
IV (2 months) (Month XI e XII)	19. Availability of the HISC4All Tool 20. Communication & Dissemination Plan + Website 21. Implementation Plan 22. Final Report	-	-	<i>SegInfo Framework and Cybersecurity.</i> <i>Final Framework</i> <i>Application Process</i> <i>Implementation Plan</i> <i>Communication & Dissemination Plan</i> <i>Final Project Report.</i> <i>(Outputs: Framework v3.0, Application Process, Operation Process and Final Training, Awareness and Training Program for the implementation and Operation of the Framework).</i>

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). 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):

- (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 (eg 1 to 3; 1 to 5; 1 to 7) with transition criteria identified and rationale specified.
- (2) The security controls to be implemented must be selected from the 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 implementation process will be guided by the following five main phases (Figure 8): (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.

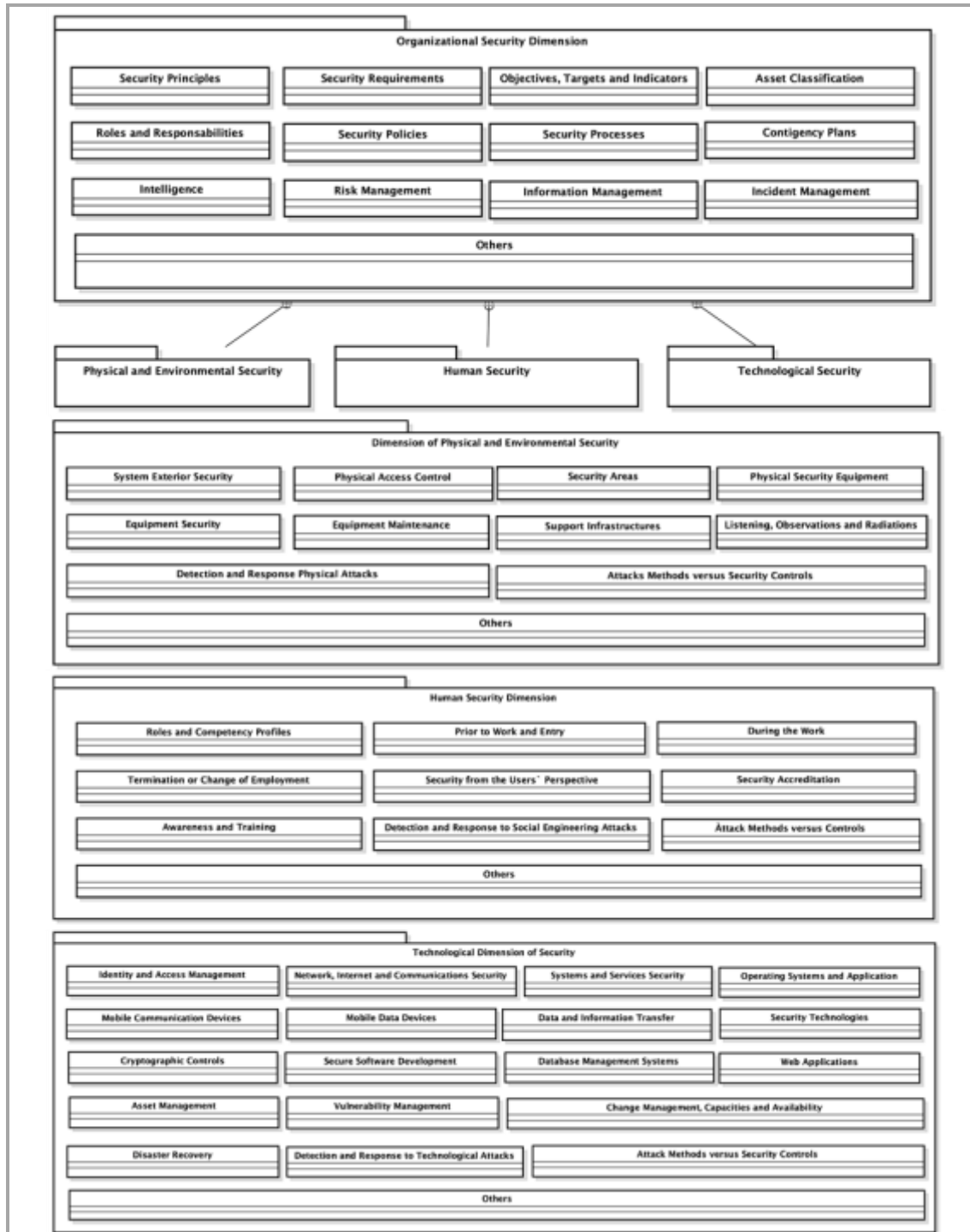


Figure 7 – Information Security and Cybersecurity Framework (Overview)

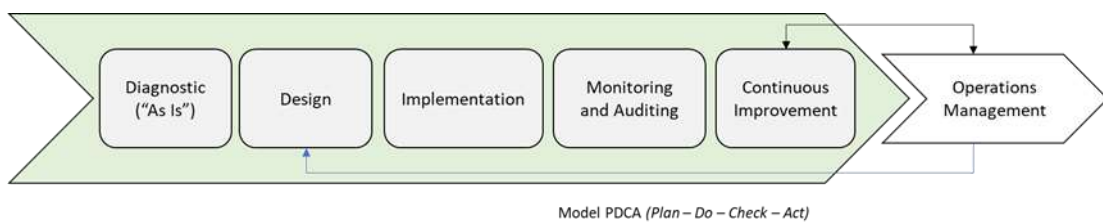


Figure 8 – General Framework Design, Implementation and Operation Process

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.



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

Continue to develop the HISC4ALL.

Activity 9. Training, Awareness and Training Program in the implementation and operation of the Framework (v1.0).

Conceiving the capacity & training activities that should be developed to consolidate the implementation of the Framework.

Activity 10. Framework Support Application

Conceive the framework support application.

Activity 11. Website

Develop a first version of the website.

Activity 12. Market Self Assessment (II)

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

Phase III. CONCEPTION & APPLICATION

Activity 13. Design of the framework application process.



Conceive the framework application process.

Activity 14. Application of the framework to health entities (Action Research – a single cycle)

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

Activity 15. Collection of lessons learned.

Register and incorporate the final remarks/suggestions.

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

Activity 17. HISC4ALL update

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

Activity 18. Market Validation + Website

Make a final validation and upgrade of the website.

PHASE IV. DISSEMINATION

Activity 19. Availability of the HISC4ALL Tool

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

Activity 20. 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 21. 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 22. 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

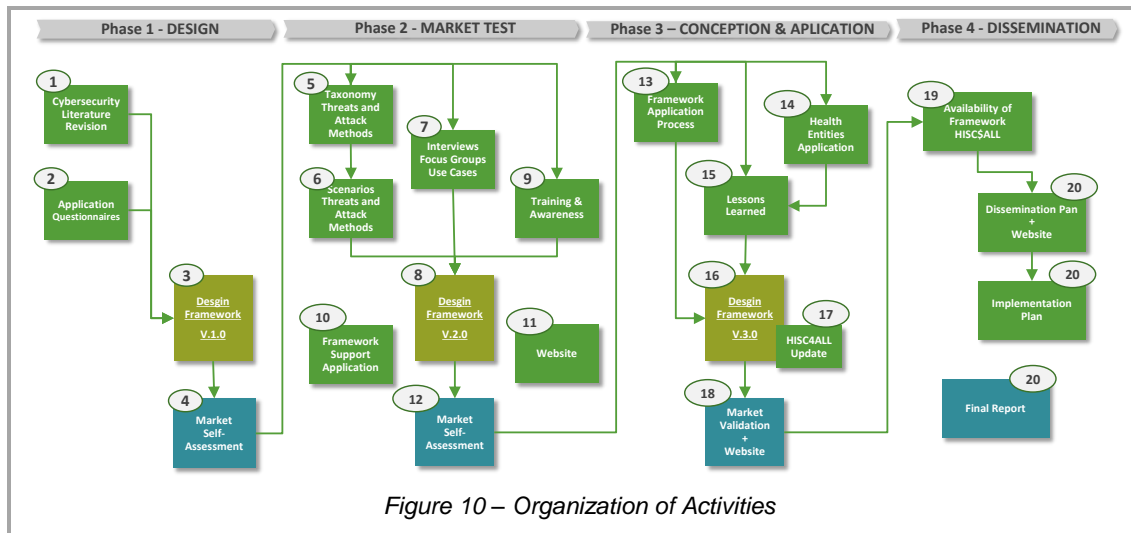


Figure 10 – Organization of Activities

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.

PDCA Model

As already mentioned, the Framework implementation process will be guided by the following main phases of the PDCA model:

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

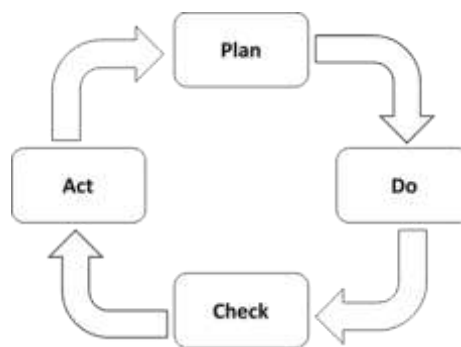


Figure 11 – Project Management Model

Risk Management Model

The risk management model adopted will be as follows:

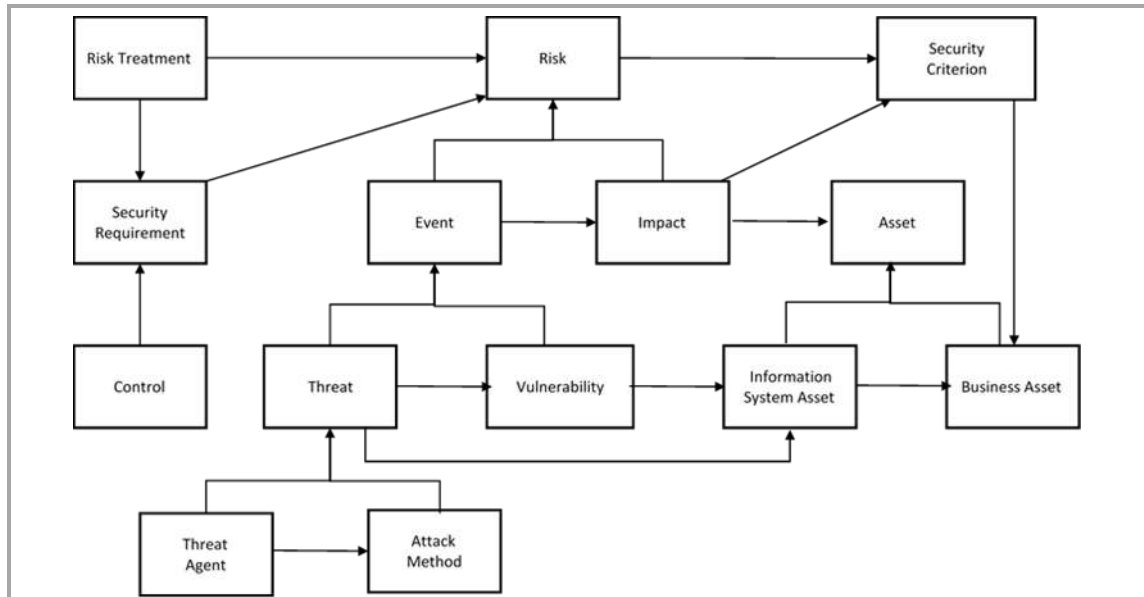


Figure 12 – Risk Management Model

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.

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;
- 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, Quattro, 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.

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		Responsibilities
INEM Pahldata	Members of the Board of Directors Project Director	<u>Decision and leadership:</u> <ul style="list-style-type: none"> - 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		Responsibilities
INEM Pahldata	Project Director Project Managers	<u>Guidance, control and management:</u> <ul style="list-style-type: none"> - 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		Responsibilities
INEM Pahldata External consultants	Functional Consultants Technical Consultants	<u>Execution:</u> <ul style="list-style-type: none"> - Performs the activities provided in the work plan, in accordance with the methodology and quality standards adopted - Prepares project documents and deliverables <p>Functional consultants:</p> <ul style="list-style-type: none"> - Collaboration in the definition and design of the solution - Support documentation preparation <p>Technical consultants:</p> <ul style="list-style-type: none"> - Solution architecture design - Integration processes definition

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

Meeting	Frequency	Responsibility	Participants
<i>Steering committee</i>	<i>Monthly</i>	<i>Steering committee</i>	<i>Steering committee</i>

<i>Kick-off</i>	<i>Single meeting</i>	<i>Project management</i>	<i>Project director Project manager Consultants Stakeholders</i>
<i>Project management</i>	<i>Biweekly</i>	<i>Project director</i>	<i>Project director Project manager</i>
<i>Project follow-up</i>	<i>Weekly</i>	<i>Project manager</i>	<i>Project manager Functional consultants</i>
<i>Technical and functional</i>	<i>Ad-hoc</i>	<i>Project manager</i>	<i>Project manager Project team</i>

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 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.

INEM 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

INEM 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.

INEM 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, a prestige healthcare entity 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
<i>Paulo Pinto</i> Project Manager	INEM	The Project Manager coordinates the teams, activities, and responsibilities of the respective Consortium Member.
<i>Filipe Botas</i> 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.
<i>José Ferreira</i> 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.
<i>Gustavo Oliveira,</i> 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.
<i>To be defined</i> 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.
<i>To be defined</i> 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.
<i>To be defined</i> 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.
<i>To be defined</i> 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 from the healthcare sector.
<i>Cátia Pinto,</i> 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: <ul style="list-style-type: none"> • Alignment of the project with the defined objectives • Strategic decision making • Evaluation of the project's evolution
<i>Filipa Correia,</i> Project Manager	Pahldata	The Project Manager coordinates the teams, activities, and responsibilities of the respective Consortium Member. This person will have the following responsibilities: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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
<i>To be defined,</i> 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: <ul style="list-style-type: none"> • Coordination and execution of the design of Outputs • Framework Implementation Process Coordination (Action Research) Assure the execution of the following tasks: <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 Modelling Techniques
<i>To be defined,</i> 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: <ul style="list-style-type: none"> • Coordination and execution of the design of Outputs • Framework Implementation Process Coordination (Action Research) Assure the execution of the following tasks: <ul style="list-style-type: none"> • Literature review and document analysis of the main national and international approaches to Information Security and Cybersecurity



		<ul style="list-style-type: none"> • Use cases / UML • Review and validation of project outputs • Support for reporting <p>Expertise</p> <ul style="list-style-type: none"> • 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 Modelling Techniques
<i>To be defined</i> Junior Information Security and Cyber Security Expert	Pahldata	<p>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.</p> <p>This person will have the following responsibilities:</p> <ul style="list-style-type: none"> • Coordination and execution of the design of Outputs • Framework Implementation Process Coordination (Action Research) <p>Assure the execution of the following tasks:</p> <ul style="list-style-type: none"> • 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 <p>Expertise</p> <ul style="list-style-type: none"> • 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 Modelling Techniques
<i>To be defined</i> Senior IT Specialist	Pahldata	<p>The Senior IT Specialist creates and provide for documentation related to system configurations, mapping, processes, and application management.</p> <p>Assure the execution of the following tasks:</p> <ul style="list-style-type: none"> • 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., BonitaBPM) • OO Database Management System (eg MongoDB) • Support for reporting
<i>To be defined</i> Junior IT Specialist	Pahldata	<p>The Junior IT Specialist creates and provide for documentation related to system configurations, mapping, processes, and application management.</p> <p>Assure the execution of the following tasks:</p> <ul style="list-style-type: none"> • 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
<i>Marta Cannas,</i> Senior	Pahldata	<p>Senior consultant that will assure the execution of the following tasks:</p>

Healthcare Expert		<ul style="list-style-type: none"> • 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 <p>Academic background on Biomedical Engineer or similar with more than five year of experience on healthcare consulting.</p>
<i>Mariana Santos,</i> Junior Healthcare Expert	Pahldata	<p>Junior consultant that will execute the following tasks:</p> <ul style="list-style-type: none"> • 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 <p>Academic background on Biomedical Engineer or similar with more than one year of experience on healthcare consulting.</p>
<i>Ana Fonseca,</i> Junior Healthcare Expert	Pahldata	<p>Junior consultant that will execute the following tasks:</p> <ul style="list-style-type: none"> • 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 <p>Academic background on Biomedical Engineer or similar with more than one year of experience on healthcare consulting.</p>

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

Assisting & Monitoring Projeto Development & Follow up, including:

- 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
- Support the conception of the website;
- Support the structuring and development of the Communication & Implementation Plans.
- Guarantee the quality control of the phases 2, 3 and 4 reports.

Another organizations

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

- Incorporate in the framework 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;
- Support the management process of implementing the wide market testing all along the 24 months of 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).

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 and Pahldata has as its object the execution of the HISC4All - Health Information Safe and Cybersecured for All project.

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

Externally, it is up to the Consortium Leader, through the Project Director, to represent the interests of the Consortium Members within the scope of the project, being granted by the parties

the powers to represent the consortium in the award of the contract, in the development and execution of the project.

The Consortium 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 were 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
<p>Activity 1. Literature review and document analysis of the main national and international approaches to Information Security and Cybersecurity</p> <p>Activity 2. Application of questionnaires and interviews to the Intervening Entities.</p> <p>Activity 3. Security Controls Framework Design (v1.0): Security Dimensions and Dimensional Controls.</p> <p>Activity 4. Market Self-Assessment (I)</p>	<p>Activity 5. Analyse, obtain or develop a taxonomy of threats/attack methods.</p> <p>Activity 6. Build and describe the main attack method scenarios / scenarios</p> <p>Activity 7. Perform the Interviews: Focus Group (Uses Cases and requirements specification).</p> <p>Activity 8. Design of the Security Controls Framework (v2.0): baselines by security dimension and control maturity levels.</p> <p>Activity 9. Training, Awareness and Training Program</p> <p>Activity 10. Framework Support Application</p> <p>Activity 11. Website</p> <p>Activity 12. Market Self Assessment (II)</p>	<p>Activity 13. Design of the framework application process.</p> <p>Activity 14. Application of the framework to health entities (Action Research – a single cycle)</p> <p>Activity 15. Collection of lessons learned.</p> <p>Activity 16. Design of the security controls framework (v3.0): security dimensions and controls by dimension.</p> <p>Activity 17. HISC4ALL Update</p> <p>Activity 18. Market Validation + Website</p>	<p>Activity 16. Availability of Framework HISC4ALL</p> <p>Activity 17. Communication & Dissemination Plan + Website</p> <p>Activity 16. Implementation Plan</p> <p>Activity 22 Final Report</p>

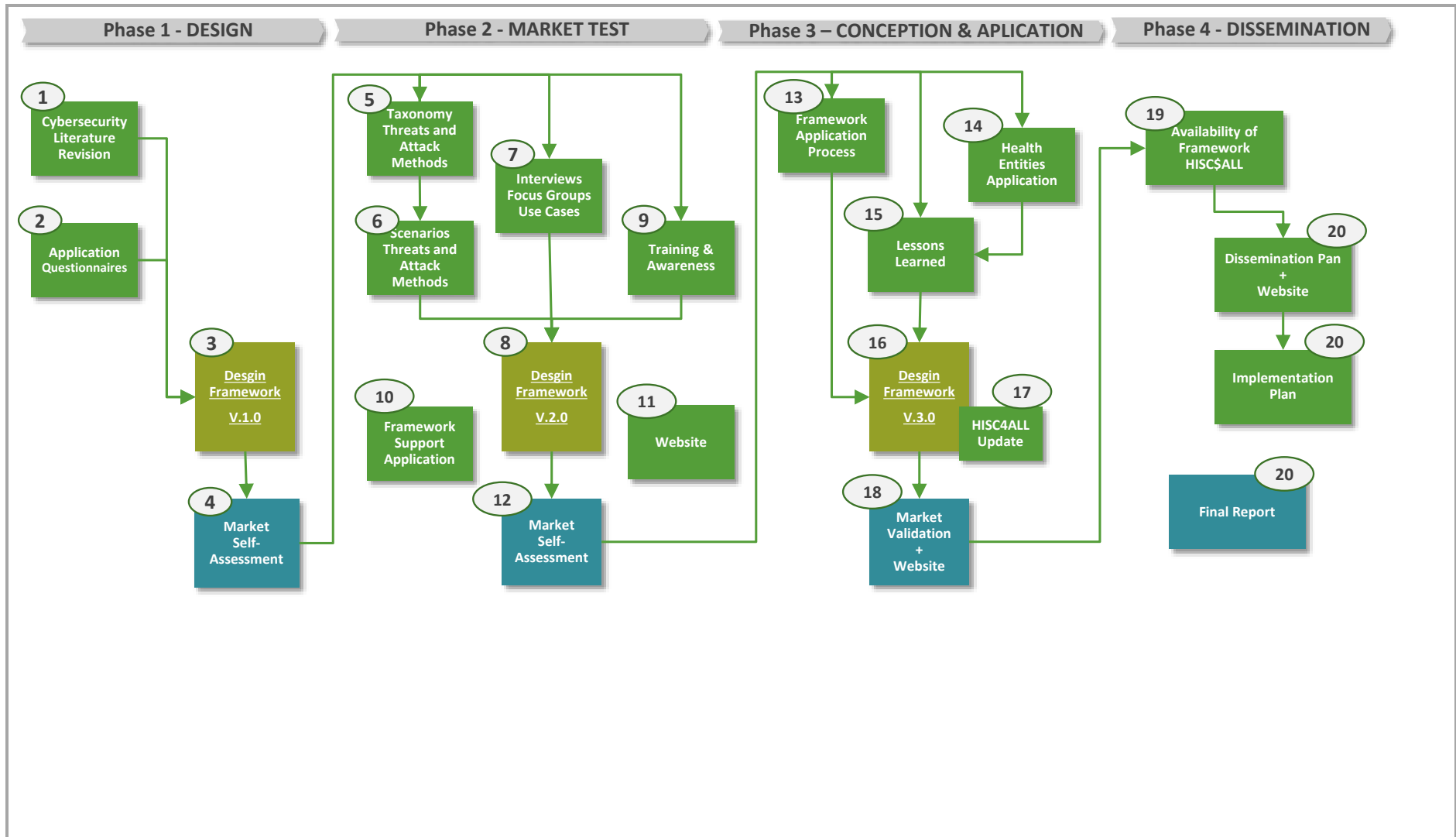
Figure 13 – Project Phases and Activities

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 (1 ^o 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).	<i>SegInfo and Cyber controls framework</i> * (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 (2 ^o 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).	<i>Framework Application Process</i> (v1.0). <i>Security Controls Framework</i> (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	-	-	<i>SegInfo Framework and Cybersecurity. Final Framework</i> <i>Application Process</i> 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).



4.2 Timetable

Timetable (projects up to 2 years)																									
<i>Fill in cells in beige to show the duration of activities. Repeat lines/columns as necessary.</i>																									
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 - Framework 2.0						■	■	■	■																
Task 9 - Training Aware.									■	■															
Task 10 - Fram Support										■	■														
Task 11 - Website											■	■													
Task 12 - Market Test												■													
Task 13 - Fram Applic													■												

2 and 3	2	Assisting & Monitoring Projeto Development & Follow up	5 to 12 and 13 to 18	20 295 EUR (50% per WP)	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	3	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
2	4	Support the development Market Tests	5 to 12	30 750 EUR	Entity to support the carrying out of Market tests and consultation of stakeholders	Continuous and permanent monitoring of compliance with the Specifications
<p>Other issues:</p> <p><i>If subcontracting for the entire project goes beyond 30% of the total eligible costs, give specific reasons.</i></p>			<p>There are no Activities subcontracted.</p> <p>The indicated subcontracted entities will develop specific activities all along the project implementation.</p>			

5. ANNEXES

5.1 Project Outline



Project
HISC4ALL
Health Information Safe and Cybersecured for All

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

Lisbon, May 2022



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:

| Europe DIGITAL | 1

1. INTRODUCTION

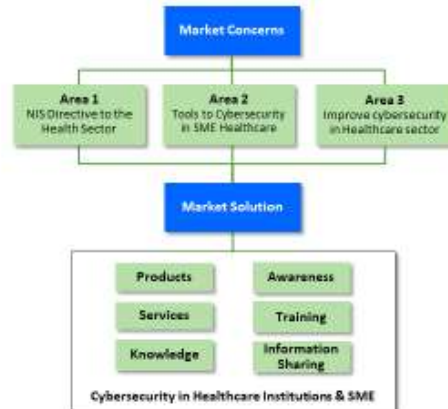
Project HISC4ALL

The project **HISC4ALL - Health Information Safe and Cybersecured for All**, to be developed by Consortium INEM-Lusiadas-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.



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.



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:

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.

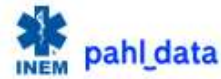
Derived Question 2: DIMENSIONS AND CATEGORIES OF CONTROLS on Information Security and Cybersecurity to be implemented. *Supported* by a literature review focused on the main general approaches to Information Security and Cybersecurity that exist and on the specifications associated with the health sector.

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).



3. PROMOTERS & TARGET STAKEHOLDERS

Application of the Solution to Market



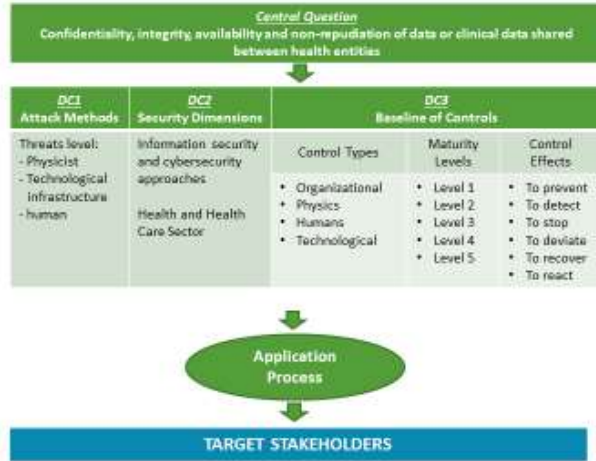
Promoters

- Instituto Nacional de Emergência Médica (INEM) – Public Institution from the Ministry of Health, responsible for the Integrated Medical Emergency System.
- Hospital Lusíadas, Private Hospital.
- QUATTRO – Private SME, Health Sector Information Solutions Provider

Target Stakeholders

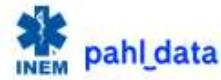
- Hospital and Clinics;
- Institutions of the Public National Health Service (NHS);
- SMEs of the healthcare sector (small hospitals, clinics, dentists, pharmacies);
- Non-profit organizations (Firefighters).

Framework



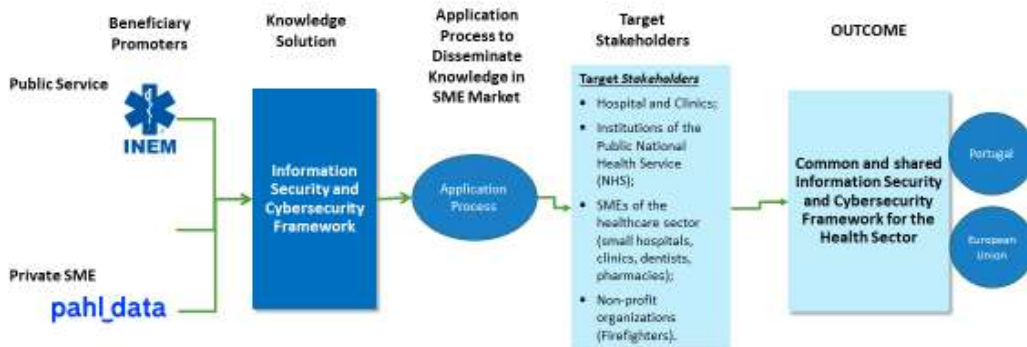
4. SCOPE & FOCUS

Type of Action



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.



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 security and cybersecurity;*
- *Promote the implementation of controls associated with information security and cybersecurity in the healthcare 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
<p>Activity 1. Literature review and document analysis of the main national and international approaches to Information Security and Cybersecurity</p> <p>Activity 2. Application of questionnaires and interviews to the Intervening Entities.</p> <p>Activity 3. Security Controls Framework Design (v1.0): Security Dimensions and Dimensional Controls.</p> <p>Activity 4. Market Self-Assessment (I)</p>	<p>Activity 5. Analyse, obtain or develop a taxonomy of threats/attack methods.</p> <p>Activity 6. Build and describe the main attack method scenarios / scenarios</p> <p>Activity 7. Perform the Interviews: Focus Group (Uses Cases and requirements specification).</p> <p>Activity 8. Design of the Security Controls Framework (v2.0): baselines by security dimension and control maturity levels.</p> <p>Activity 9. Training, Awareness and Training Program</p> <p>Activity 10. Framework Support Application</p> <p>Activity 11. Website</p> <p>Activity 12. Market Self Assessment (II)</p>	<p>Activity 13. Design of the framework application process.</p> <p>Activity 14. Application of the framework to health entities (Action Research – a single cycle)</p> <p>Activity 15. Collection of lessons learned.</p> <p>Activity 16. Design of the security controls framework (v3.0): security dimensions and controls by dimension.</p> <p>Activity 17. HISC4ALL Update</p> <p>Activity 18. Market Validation + Website</p>	<p>Activity 16. Availability of Framework HISC4ALL</p> <p>Activity 17. Communication & Dissemination Plan + Website</p> <p>Activity 16. Implementation Plan</p> <p>Activity 22 Final Report</p>



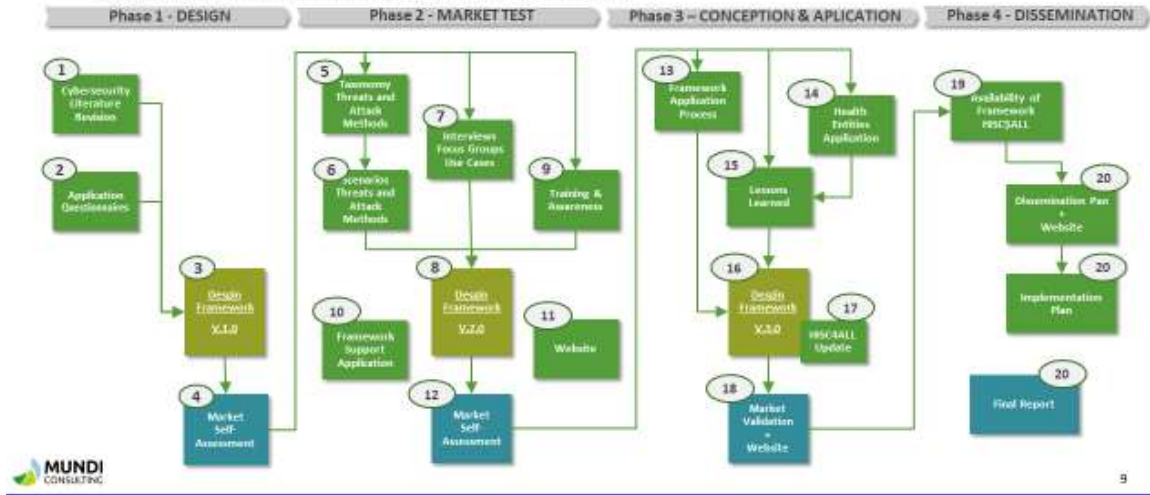
8

6. PHASES & ACTIVITIES

Organization of Activities

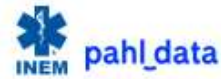


Organization of the development of Activities in each of the Phases:



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



8. TIMETABLE

Project development schedule



Schedule to develop the project activities:

1. DESIGN	2. MARKET TEST	3. CONCEPTION & APPLICATION	4. DISSEMINATION
<p>Activity 1. Literature review and document analysis of the main national and international approaches to Information Security and Cybersecurity</p> <p>Activity 2. Application of questionnaires and interviews to the Intervening Entities.</p> <p>Activity 3. Security Controls Framework Design (v1.0): Security Dimensions and Dimensional Controls.</p> <p>Activity 4. Market Self-Assessment (I)</p>	<p>Activity 5. Analyse, obtain or develop a taxonomy of threats/attack methods.</p> <p>Activity 6. Build and describe the main attack method scenarios / scenarios</p> <p>Activity 7. Perform the Interviews: Focus-Group (Uses Cases and requirements specification).</p> <p>Activity 8. Design of the Security Controls Framework (v2.0): baselines by security dimension and control-maturity levels.</p> <p>Activity 9. Training, Awareness and Training Program</p> <p>Activity 10. Framework Support Application.</p> <p>Activity 11. Website.</p> <p>Activity 12. Market Self-Assessment (II)</p>	<p>Activity 13. Design of the framework application process.</p> <p>Activity 14. Application of the framework to health entities (Action Research – a single cycle)</p> <p>Activity 15. Collection of lessons learned.</p> <p>Activity 16. Design of the security controls framework (v1.0): security dimensions and controls by dimension.</p> <p>Activity 17. HISC4ALL Update</p> <p>Activity 18. Market Validation + Website</p>	<p>Activity 16. Availability of Framework HISC4ALL</p> <p>Activity 17. Communication & Dissemination Plan + Website</p> <p>Activity 18. Implementation Plan</p> <p>Activity 22. Final Report</p>
4 Months	8 Months	10 Months	2 Months

2 Years



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

SUBCONTRACTOR

Management Consultancy Partner



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

5.2 Presentation of the Figures presented in the Formulaire

Figure 1 – Framework Configuration

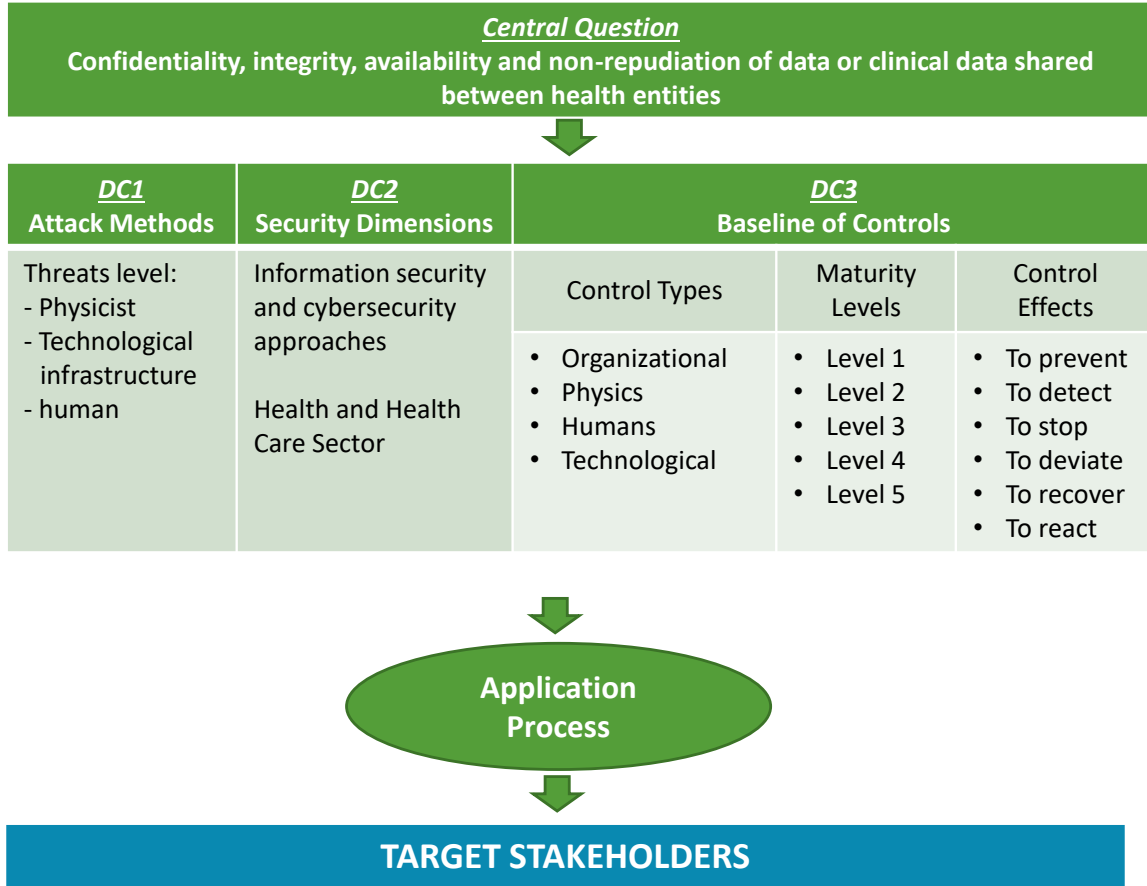


Figure 2 – Use Cases: Project Vision

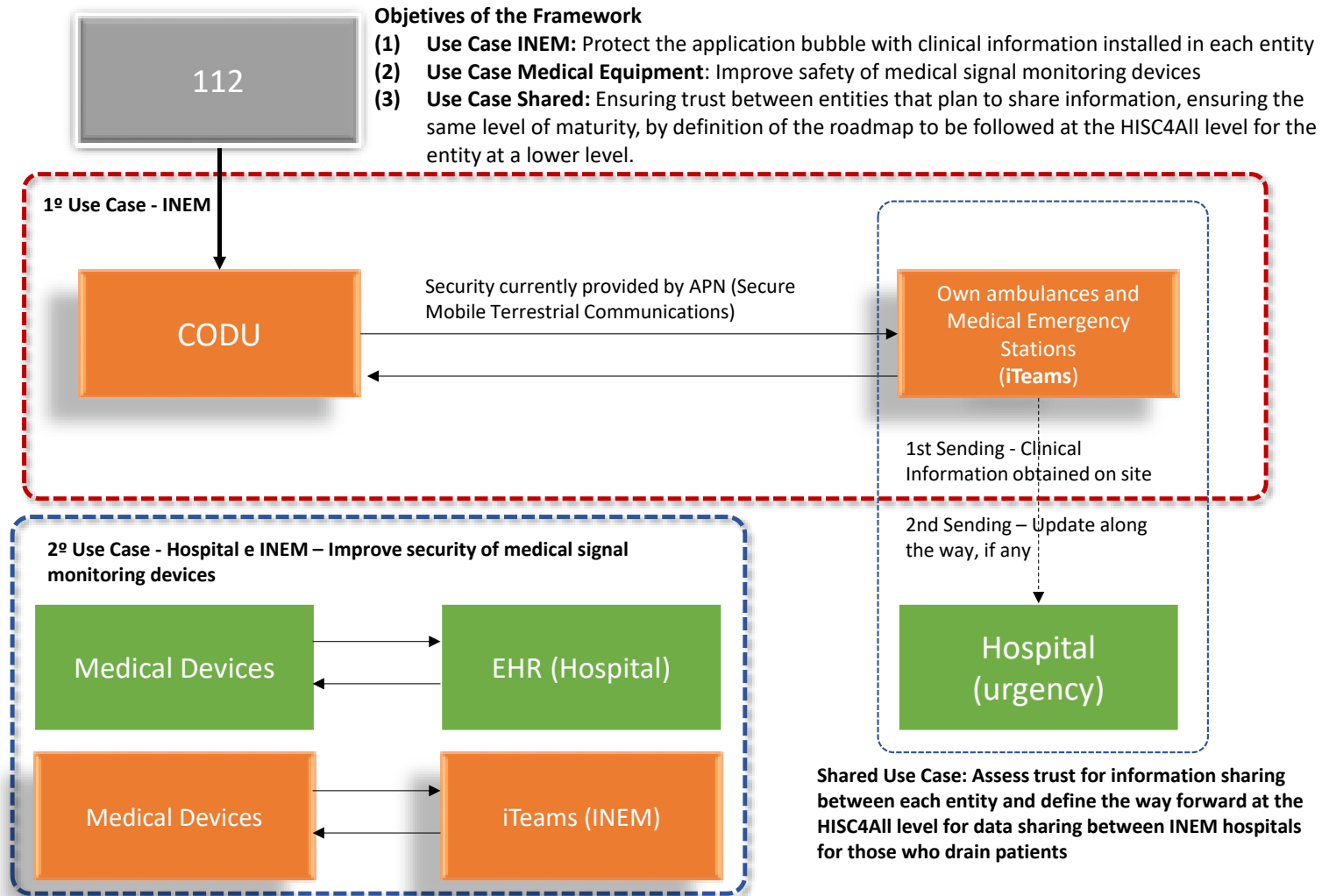


Figure 2 – Use Cases: Project Vision

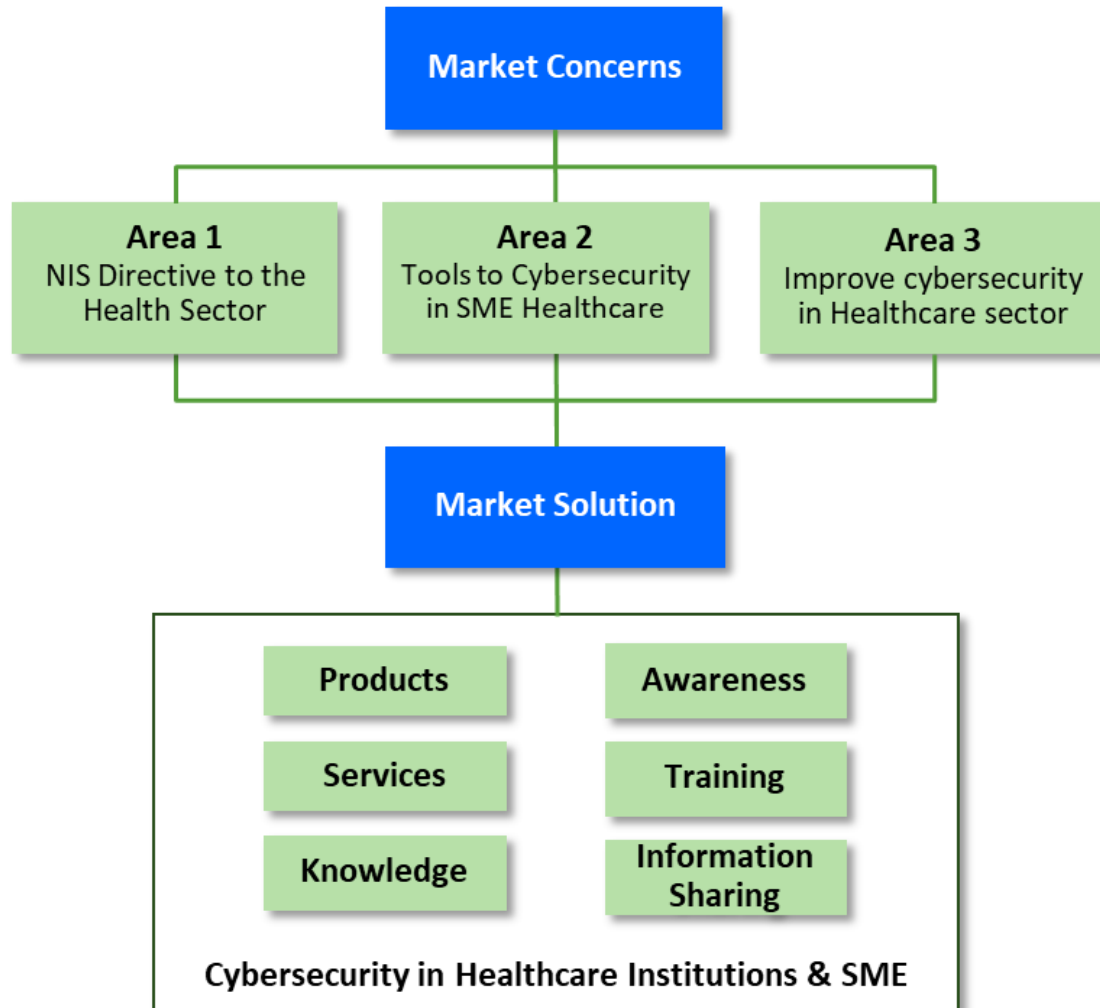


Figure 3 – Introduction of the Framework in the Market

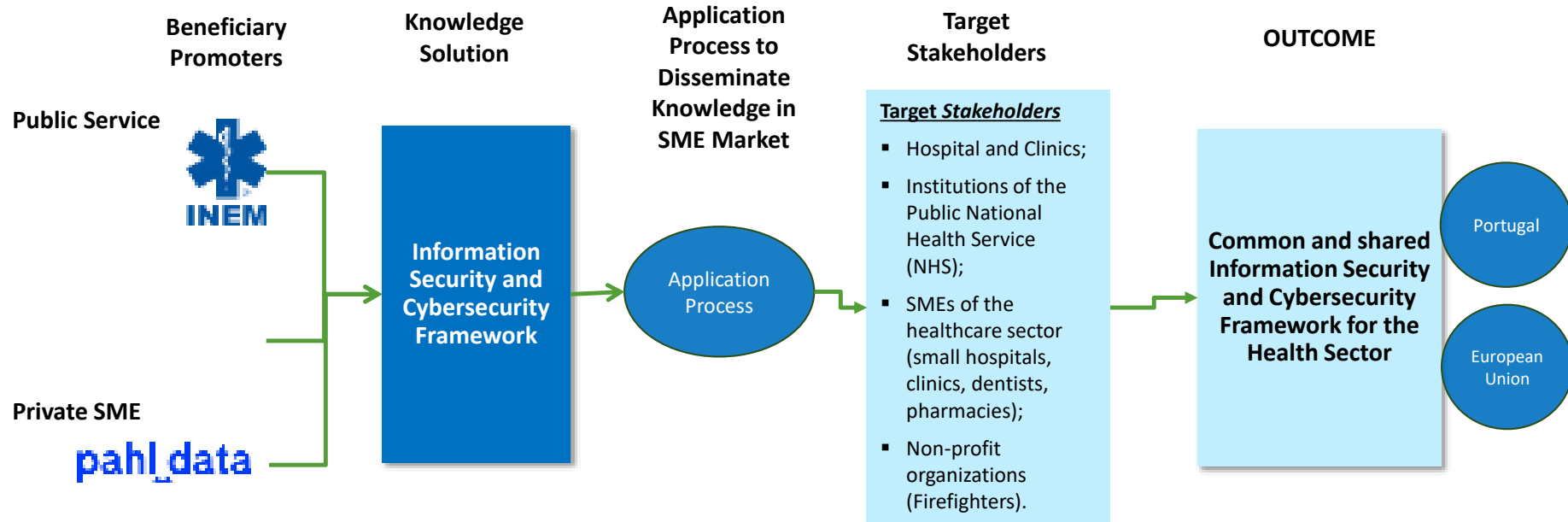


Figure 4 – Use Cases: Project Vision

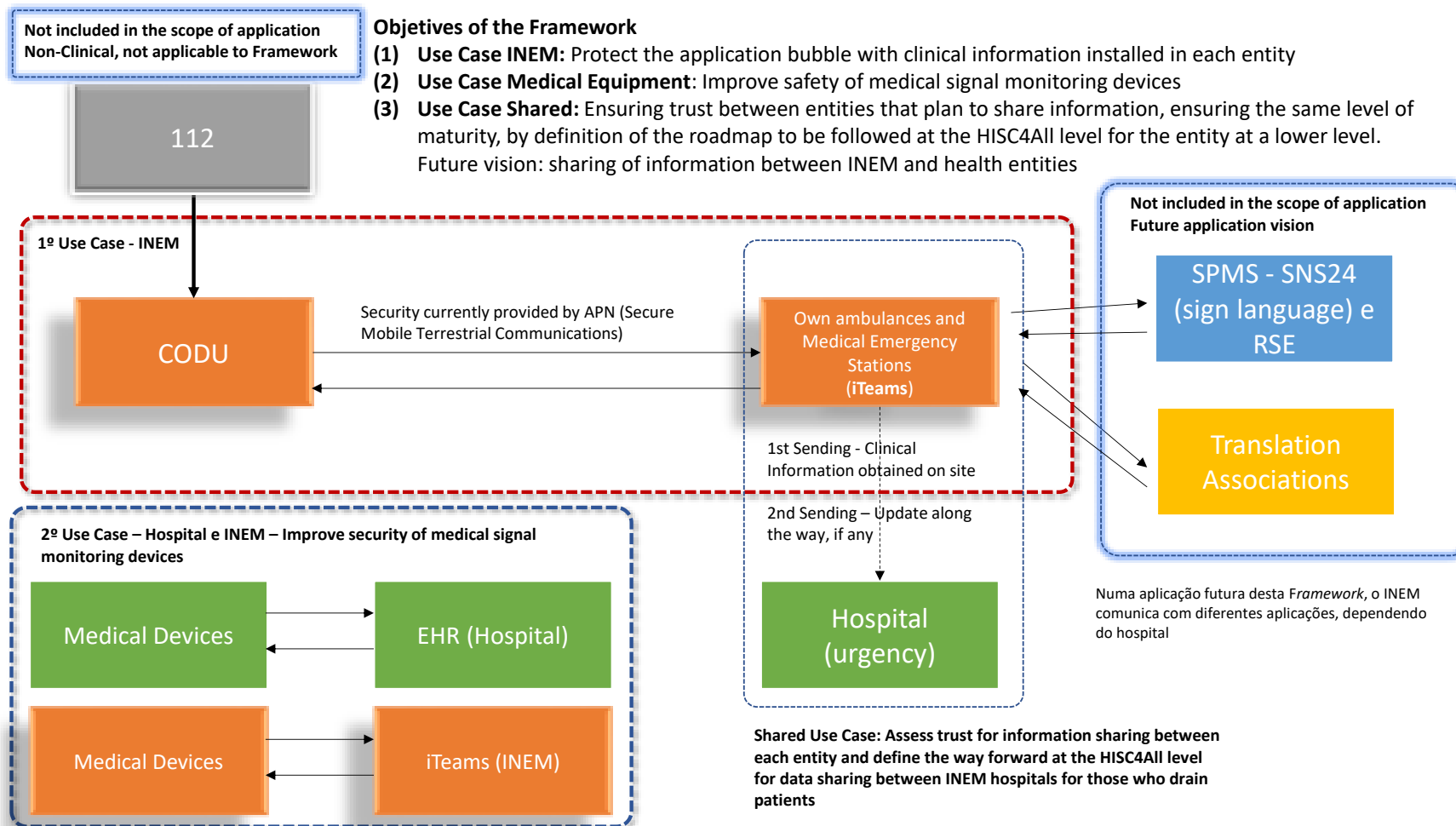


Figure 5 – Project General Working Plan – First Year

Project General Working Plan				
Phases (1 ^o 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)	<ul style="list-style-type: none"> - National / international standards and references. - Elements for application of questionnaires and interviews. 	<ul style="list-style-type: none"> - Delay in applying questionnaires and conducting interviews (Low Risk). 	<i>SegInfo and Cyber controls framework</i> * (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)	<ul style="list-style-type: none"> - 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 	<ul style="list-style-type: none"> - 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 6 – Project General Working Plan – Second Year



Project General Working Plan (cont.)				
Phases (2^o 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	<ul style="list-style-type: none"> - International standards. - Entities / Organizations to apply the framework (<i>proof of concept: one baseline per dimension of the framework</i>) 	<ul style="list-style-type: none"> - Availability of Entities /Organizations to apply the framework (Low Risk). 	<i>Framework Application Process (v1.0).</i> <i>Security Controls Framework (v3.0).</i> <i>Partial report of project no. 3.</i> <i>(Outputs: Framework v3.0 and Application Process)</i>
IV (2 months) (Month XI e XII)	19. Availability of the HISC4All Tool 20. Communication & Dissemination Plan + Website 21. Implementation Plan 22. Final Report	-	-	<i>SegInfo Framework and Cybersecurity.</i> <i>Final Framework</i> <i>Application Process</i> <i>Implementation Plan</i> <i>Communication & Dissemination Plan</i> <i>Final Project Report.</i> <i>(Outputs: Framework v3.0, Application Process, Operation Process and Final Training, Awareness and Training Program for the implementation and Operation of the Framework).</i>

Figure 7 – Information Security and Cybersecurity Framework (Overview)

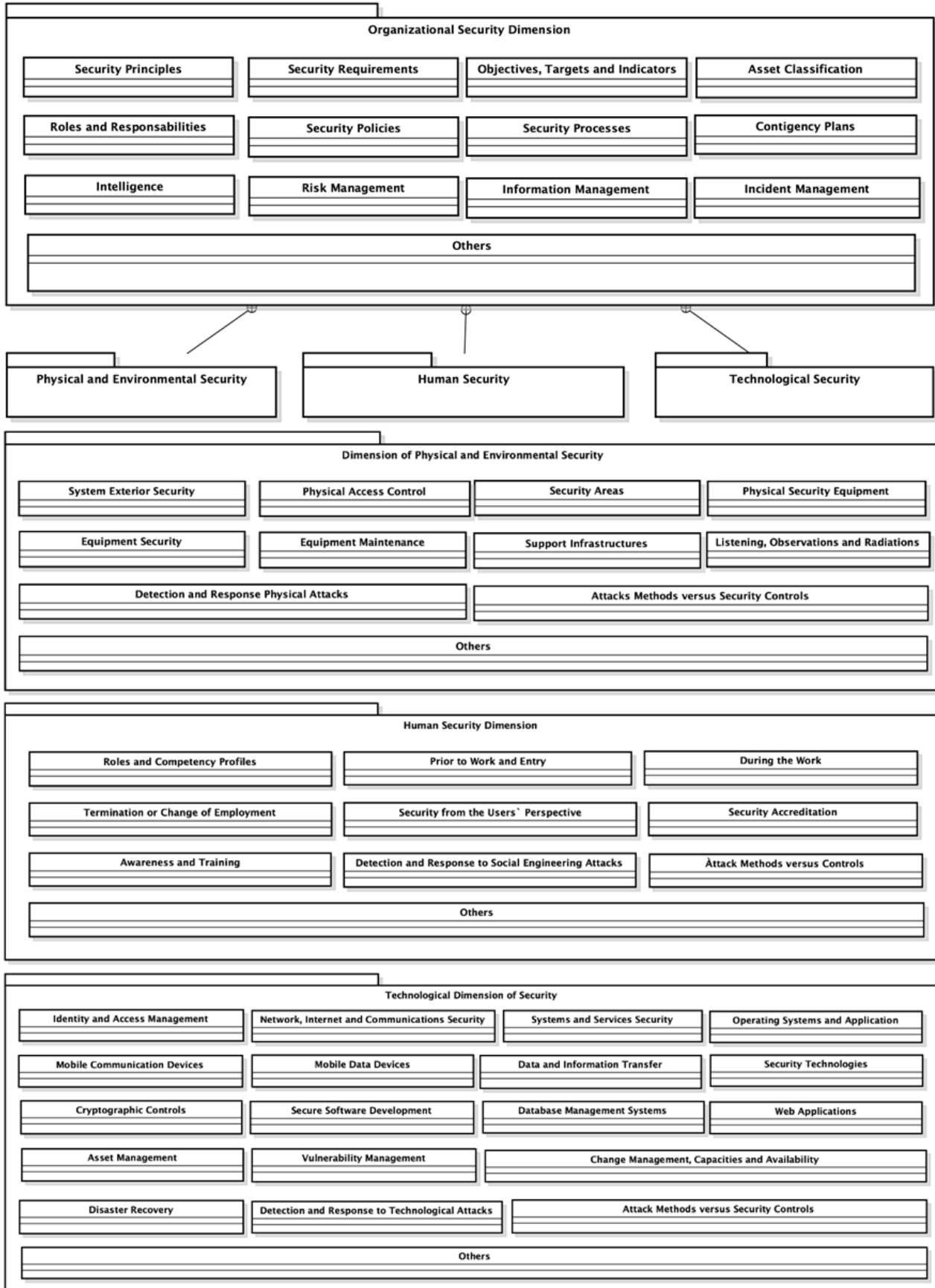


Figure 8 – General Framework Design, Implementation and Operation Process

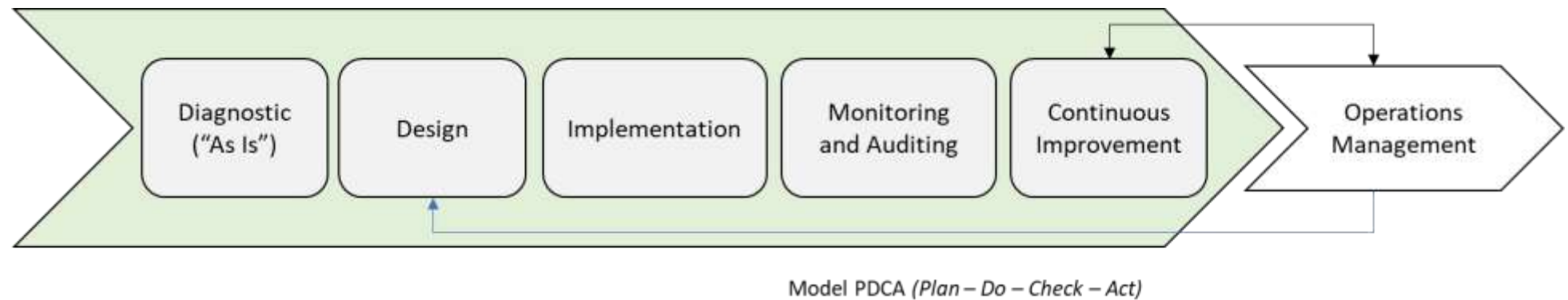


Figure 9 – Training, Awareness and Training Program

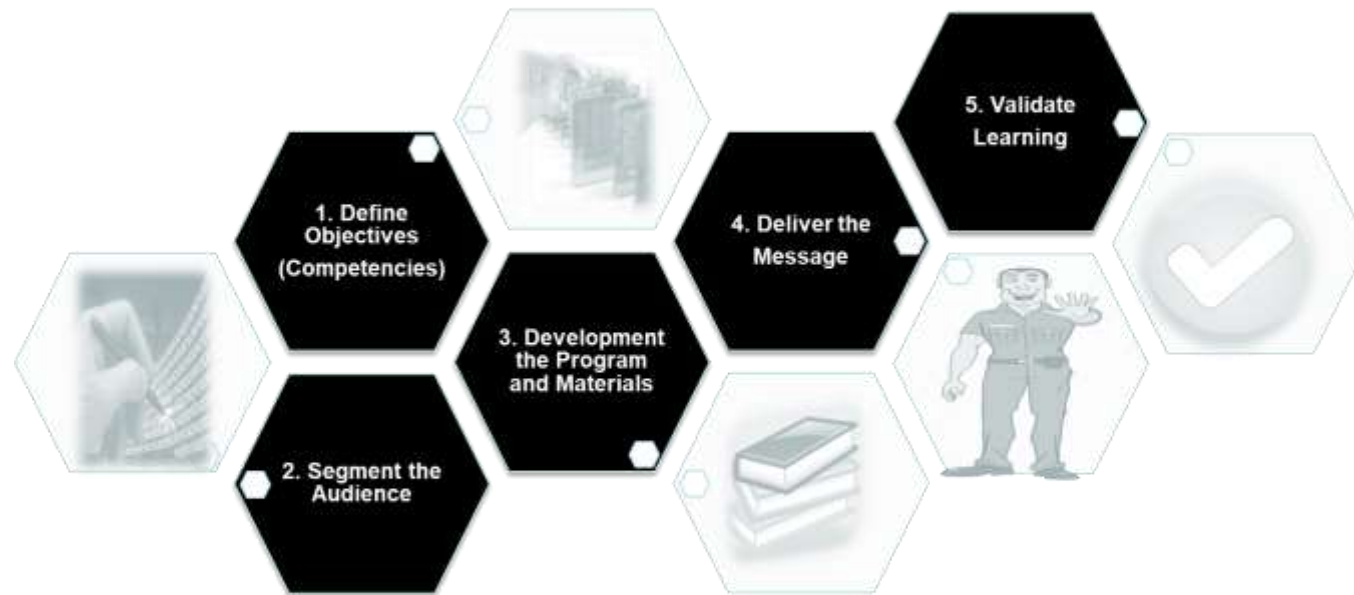


Figure 10 – Organization of Activities

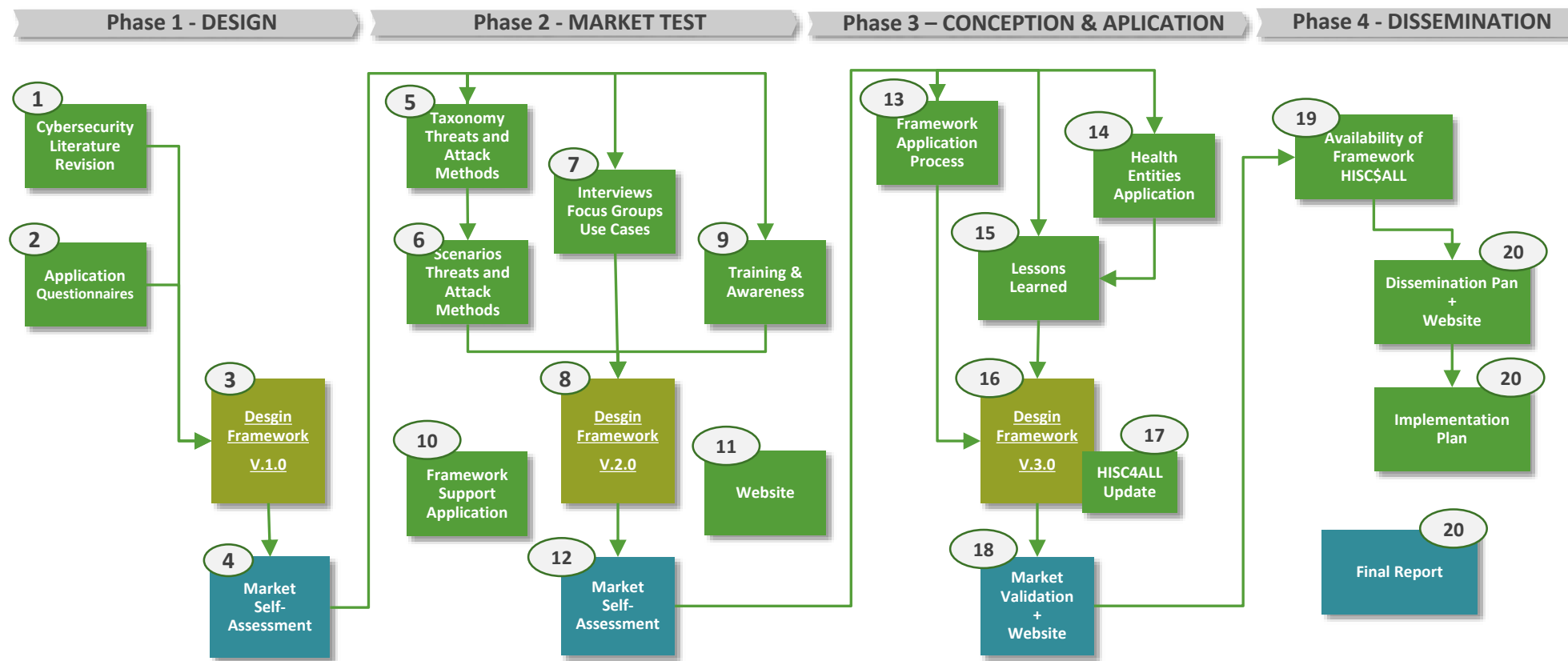


Figure 11 – Project Management Model

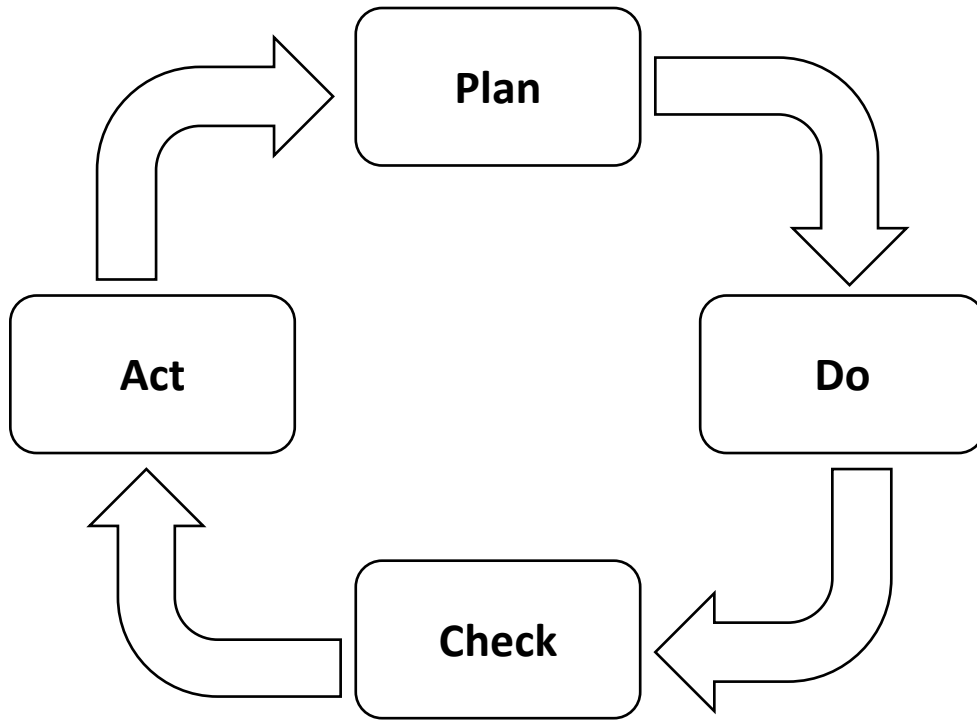


Figure 12 – Risk Management Model

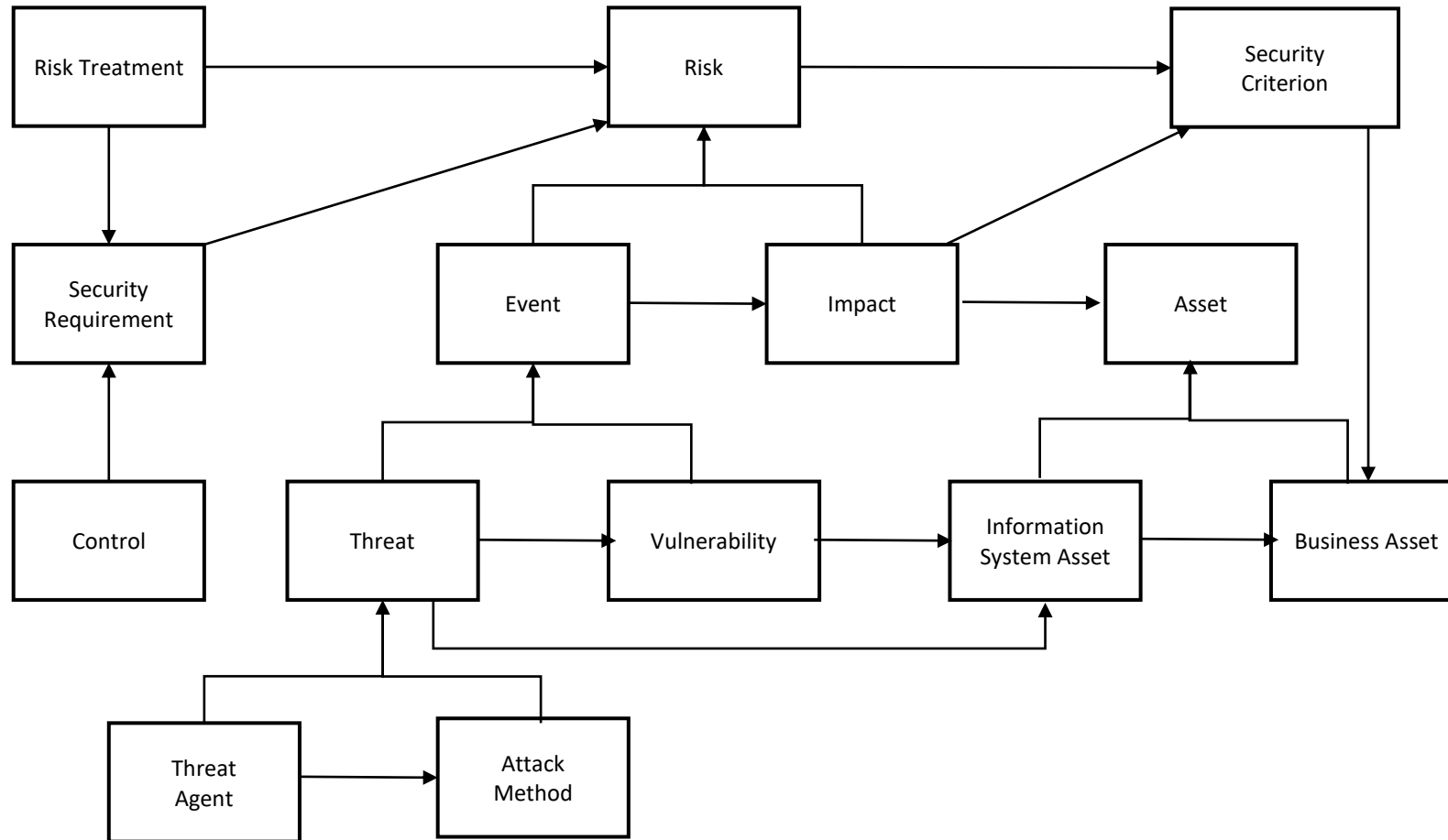


Figure 13 – Project Phases and Activities

1. DESIGN	2. MARKET TEST	3. CONCEPTION & APPLICATION	4. DISSEMINATION
<p>Activity 1. Literature review and document analysis of the main national and international approaches to Information Security and Cybersecurity</p> <p>Activity 2. Application of questionnaires and interviews to the Intervening Entities.</p> <p>Activity 3. Security Controls Framework Design (v1.0): Security Dimensions and Dimensional Controls.</p> <p>Activity 4. Market Self-Assessment (I)</p>	<p>Activity 5. Analyse, obtain or develop a taxonomy of threats/attack methods.</p> <p>Activity 6. Build and describe the main attack method scenarios / scenarios</p> <p>Activity 7. Perform the Interviews: Focus Group (Uses Cases and requirements specification).</p> <p>Activity 8. Design of the Security Controls Framework (v2.0): baselines by security dimension and control maturity levels.</p> <p>Activity 9. Training, Awareness and Training Program</p> <p>Activity 10. Framework Support Application</p> <p>Activity 11. Website</p> <p>Activity 12. Market Self Assessment (II)</p>	<p>Activity 13. Design of the framework application process.</p> <p>Activity 14. Application of the framework to health entities (Action Research – a single cycle)</p> <p>Activity 15. Collection of lessons learned.</p> <p>Activity 16. Design of the security controls framework (v3.0): security dimensions and controls by dimension.</p> <p>Activity 17. HISC4ALL Update</p> <p>Activity 18. Market Validation + Website</p>	<p>Activity 16. Availability of Framework HISC4ALL</p> <p>Activity 17. Communication & Dissemination Plan + Website</p> <p>Activity 16. Implementation Plan</p> <p>Activity 22 Final Report</p>



HISTORY OF CHANGES		
VERSION	PUBLICATION DATE	CHANGE
1.0	23.09.2022	Initial version.
2.0	09.12.2022	Second version

ANNEX 2a

ADDITIONAL INFORMATION ON UNIT COSTS AND CONTRIBUTIONS

SME owners/natural person beneficiaries without salary (Decision C(2020) 7115¹)

Type: unit costs

Units: days spent working on the action (rounded up or down to the nearest half-day)

Amount per unit (daily rate): calculated according to the following formula:

{EUR 5 080 / 18 days = **282,22**}
multiplied by
{country-specific correction coefficient of the country where the beneficiary is established}

The country-specific correction coefficients used are those set out in the Horizon Europe Work Programme (section Marie Skłodowska-Curie actions) in force at the time of the call (see [Portal Reference Documents](#)).

¹ Commission [Decision](#) of 20 October 2020 authorising the use of unit costs for the personnel costs of the owners of small and medium-sized enterprises and beneficiaries that are natural persons not receiving a salary for the work carried out by themselves under an action or work programme (C(2020)7715).

ANNEX 3

ACCESSION FORM FOR BENEFICIARIES

PAHLDATA (PORTUGAL) - COMERCIO DE EQUIPAMENTO DE INFORMATICA S.A. (PAHLDATA), PIC 893426940, established in RUA QUINTA DO PINHEIRO N 16-3 C, CARNAXIDE 2790-143, Portugal,

hereby agrees

to become beneficiary

in Agreement No 101100701 — HISC4ALL ('the Agreement')

between INEM (INEM) and the European Union ('EU'), represented by the European Commission ('European Commission' or 'granting authority'),

and mandates

the coordinator to submit and sign in its name and on its behalf any **amendments** to the Agreement, in accordance with Article 39.

By signing this accession form, the beneficiary accepts the grant and agrees to implement it in accordance with the Agreement, with all the obligations and terms and conditions it sets out.

SIGNATURE

For the beneficiary

ANNEX 4 DIGITAL EUROPE MGA — MULTI + MONO

FINANCIAL STATEMENT FOR [PARTICIPANT NAME] FOR REPORTING PERIOD [NUMBER]

Eligible ¹ costs (per budget category)											EU contribution ²				Revenues			
Direct costs										Indirect costs	Total costs	EU contribution to eligible costs			Total requested EU contribution	Income generated by the action		
A. Personnel costs		B. Subcontracting costs	C. Purchase costs			D. Other cost categories			E. Indirect costs ²	Funding rate % ³		Maximum EU contribution ⁴	Requested EU contribution					
Forms of funding	A.1 Employees (or equivalent)	A.4 SME owners and natural person beneficiaries	B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.X Financial support to third parties	D.2 Internally invoiced goods and services	[OPTION for PAC Grants for Procurement: D.3 PAC procurement costs]	E. Indirect costs	Flat-rate costs ⁶	Total costs	Funding rate % ³	Maximum EU contribution ⁴	Requested EU contribution	Total requested EU contribution	Income generated by the action	
	A.2 Natural persons under direct contract	A.3 Seconded persons	Actual costs	Unit costs (usual accounting practices)	Unit costs ⁵	Actual costs	Actual costs	Actual costs	Actual costs	Actual costs								Unit costs (usual accounting practices)
	a1	a2	a3	b	c1	c2	c3	d1a	d2	[d3]	e = flat-rate * (a1 + a2 + a3 + b + c1 + c2 + c3 + d1a + d2 (+ d3))	f = a+b+c+d+e	U	g = f*U%	h	m	n	
XX – [short name beneficiary/affiliated entity]																		

The beneficiary/affiliated entity hereby confirms that:
 The information provided is complete, reliable and true.
 The costs and contributions declared are eligible (see Article 6).
 The costs and contributions can be substantiated by adequate records and supporting documentation that will be produced upon request or in the context of checks, reviews, audits and investigations (see Articles 19, 20 and 25).
 For the last reporting period: that all the revenues have been declared (see Article 22).

¹ Please declare all eligible costs and contributions, even if they exceed the amounts indicated in the estimated budget (see Annex 2). Only amounts that were declared in your individual financial statements can be taken into account later on, in order to replace costs/contributions that are found to be ineligible.

² See Article 6 for the eligibility conditions. All amounts must be expressed in EUR (see Article 21 for the conversion rules).

³ If you have also received an EU operating grant during this reporting period, you cannot claim indirect costs - unless you can demonstrate that the operating grant does not cover any costs of the action. This requires specific accounting tools. Please contact us immediately via the Funding & Tenders Portal for details.

⁴ See Data Sheet for the reimbursement rate(s).

⁵ This is the *theoretical* amount of EU contribution to costs that the system calculates automatically (by multiplying the reimbursement rates by the costs declared). The amount you request (in the column 'requested EU contribution') may be less.

⁶ See Annex 2a 'Additional information on the estimated budget' for the details (units, cost per unit).

⁷ See Data Sheet for the flat-rate.

ANNEX 5

SPECIFIC RULES

CONFIDENTIALITY AND SECURITY (— ARTICLE 13)

Sensitive information with security recommendation

Sensitive information with a security recommendation must comply with the additional requirements imposed by the granting authority.

Before starting the action tasks concerned, the beneficiaries must have obtained all approvals or other mandatory documents needed for implementing the task. The documents must be kept on file and be submitted upon request by the coordinator to the granting authority. If they are not in English, they must be submitted together with an English summary.

For requirements restricting disclosure or dissemination, the information must be handled in accordance with the recommendation and may be disclosed or disseminated only after written approval from the granting authority.

EU classified information

If EU classified information is used or generated by the action, it must be treated in accordance with the security classification guide (SCG) and security aspect letter (SAL) set out in Annex 1 and Decision 2015/444¹ and its implementing rules — until it is declassified.

Deliverables which contain EU classified information must be submitted according to special procedures agreed with the granting authority.

Action tasks involving EU classified information may be subcontracted only with prior explicit written approval from the granting authority and only to entities established in an EU Member State or in a non-EU country with a security of information agreement with the EU (or an administrative arrangement with the Commission).

EU classified information may not be disclosed to any third party (including participants involved in the action implementation) without prior explicit written approval from the granting authority.

ETHICS (— ARTICLE 14)

Ethics

Actions involving activities raising ethics issues must be carried out in compliance with:

- ethical principles

¹ Commission Decision 2015/444/EC, Euratom of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

and

- applicable EU, international and national law, including the EU Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Supplementary Protocols.

The beneficiaries must pay particular attention to the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of persons, the right to non-discrimination, the need to ensure protection of the environment and high levels of human health protection.

Before the beginning of an action task raising an ethical issue, the beneficiaries must have obtained all approvals or other mandatory documents needed for implementing the task, notably from any (national or local) ethics committee or other bodies such as data protection authorities.

The documents must be kept on file and be submitted upon request by the coordinator to the granting authority. If they are not in English, they must be submitted together with an English summary, which shows that the documents cover the action tasks in question and includes the conclusions of the committee or authority concerned (if any).

INTELLECTUAL PROPERTY RIGHTS (IPR) — BACKGROUND AND RESULTS — ACCESS RIGHTS AND RIGHTS OF USE (— ARTICLE 16)

Definitions

Access rights — Rights to use results or background.

Dissemination — The public disclosure of the results by appropriate means, other than resulting from protecting or exploiting the results, including by scientific or professional publications in any medium.

Exploit(ation) — The use of results in further innovation and deployment activities other than those covered by the action concerned, including among other things, commercial exploitation such as developing, creating, manufacturing and marketing a product or process, creating and providing a service, or in standardisation activities.

Fair and reasonable conditions — Appropriate conditions, including possible financial terms or royalty-free conditions, taking into account the specific circumstances of the request for access, for example the actual or potential value of the results or background to which access is requested and/or the scope, duration or other characteristics of the exploitation envisaged.

List of background — Background free from restrictions

The beneficiaries must, where industrial and intellectual property rights (including rights of third parties) exist prior to the Agreement, establish a list of these pre-existing industrial and intellectual property rights, specifying the rights owners.

The coordinator must — before starting the action — submit this list to the granting authority.

Where the call conditions restrict participation or control due to security or EU strategic autonomy reasons, background that is subject to control or other restrictions by a country (or entity from a country) which is not one of the eligible countries or target countries set out in the call conditions and that impact the results (i.e. would make the results subject to control or restrictions) must not be used and must be explicitly excluded in the list of background — unless otherwise agreed with the granting authority.

Results free from restrictions

Where the call conditions restrict participation or control due to security or EU strategic autonomy reasons, the beneficiaries must ensure that the results of the action are not subject to control or other restrictions by a country (or entity from a country) which is not one of the eligible countries or target countries set out in the call conditions — unless otherwise agreed with the granting authority.

Ownership of results

Results are owned by the beneficiaries that generate them (unless the consortium agreement specifies another ownership regime).

Protection of results

The beneficiaries must adequately protect their results — for an appropriate period and with appropriate territorial coverage — if protection is possible and justified, taking into account all relevant considerations, including the prospects for commercial exploitation, legitimate interests of the other beneficiaries and any other legitimate interests.

Exploitation of results

Beneficiaries must — up to four years after the end of the action (see Data Sheet, Point 1) — use their best efforts to exploit their results directly or to have them exploited indirectly by another entity, in particular through transfer or licensing.

Where the call conditions restrict participation or control due to security or EU strategic autonomy reasons (and unless otherwise agreed with the granting authority), the beneficiaries must produce a significant amount of products, services or processes that incorporate results of the action or that are produced through the use of results of the action in the eligible countries or target countries set out in the call conditions.

Where the call conditions impose moreover a first exploitation obligation, the first exploitation must also take place in the eligible countries or target countries set out in the call conditions.

The beneficiaries must ensure that these obligations also apply to their affiliated entities, associated partners, subcontractors and recipients of financial support to third parties.

Transfers and licensing of results

Where the call conditions restrict participation or control due to security or EU strategic autonomy reasons, the beneficiaries may not transfer ownership of their results or grant licences to third parties which are established in countries which are not eligible countries or target countries set out in the call conditions (or are controlled by such countries or entities

from such countries) — unless they have requested and received prior approval by the granting authority.

The request must:

- identify the specific results concerned
- describe in detail the new owner and the planned or potential exploitation of the results and
- include a reasoned assessment of the likely impact of the transfer or license on the security interests or EU strategic autonomy .

The granting authority may request additional information.

The beneficiaries must ensure that their obligations under the Agreement are passed on to the new owner and that this new owner has the obligation to pass them on in any subsequent transfer.

Access rights — Additional rights of use

Rights of use of the granting authority on results for information, communication, publicity and dissemination purposes

The granting authority also has the right to exploit non-sensitive results of the action for information, communication, dissemination and publicity purposes, using any of the following modes:

- **use for its own purposes** (in particular, making them available to persons working for the granting authority or any other EU service (including institutions, bodies, offices, agencies, etc.) or EU Member State institution or body; copying or reproducing them in whole or in part, in unlimited numbers; and communication through press information services)
- **distribution to the public** in hard copies, in electronic or digital format, on the internet including social networks, as a downloadable or non-downloadable file
- **editing** or **redrafting** (including shortening, summarising, changing, correcting, cutting, inserting elements (e.g. meta-data, legends or other graphic, visual, audio or text elements) extracting parts (e.g. audio or video files), dividing into parts or use in a compilation
- **translation**(including inserting subtitles/dubbing)in all official languages of EU
- **storage** in paper, electronic or other form
- **archiving** in line with applicable document-management rules
- the right to authorise **third parties** to act on its behalf or sub-license to third parties, including if there is licensed background, any of the rights or modes of exploitation set out in this provision
- **processing**, analysing, aggregating the results and **producing derivative works**

- **disseminating** the results in widely accessible databases or indexes (such as through ‘open access’ or ‘open data’ portals or similar repositories, whether free of charge or not).

The beneficiaries must ensure these rights of use for the whole duration they are protected by industrial or intellectual property rights.

If results are subject to moral rights or third party rights (including intellectual property rights or rights of natural persons on their image and voice), the beneficiaries must ensure that they comply with their obligations under this Agreement (in particular, by obtaining the necessary licences and authorisations from the rights holders concerned).

Access rights for the granting authority and EU institutions, bodies, offices or agencies to results for policy purposes

The beneficiaries must grant access to their results — on a royalty-free basis — to the granting authority, other EU institutions, bodies, offices or agencies, for developing, implementing and monitoring EU policies or programmes.

Such access rights are limited to non-commercial and non-competitive use.

Access rights for the granting authority to results in case of a public emergency

If requested by the granting authority in case of a public emergency, the beneficiaries must grant non-exclusive, world-wide licences to third parties — under fair and reasonable conditions — to use the results to address the public emergency.

Access rights for third parties to ensure continuity and interoperability

Where the call conditions impose continuity or interoperability obligations, the beneficiaries must make the results produced in the framework of the action available to the public (freely accessible on the Internet under open source licences).

COMMUNICATION, DISSEMINATION AND VISIBILITY (— ARTICLE 17)

Communication and dissemination plan

The beneficiaries must provide a detailed communication and dissemination plan, setting out the objectives, key messaging, target audiences, communication channels, social media plan, planned budget and relevant indicators for monitoring and evaluation.

Dissemination of results

The beneficiaries must disseminate their results as soon as feasible, in a publicly available format, subject to any restrictions due to the protection of intellectual property, security rules or legitimate interests.

They must upload the public **project results** to the Digital Europe Project Results platform, available through the Funding & Tenders Portal.

In addition, where the call conditions impose additional dissemination obligations, they must also comply with those.

Additional communication activities

The beneficiaries must engage in the following additional communication activities:

- **present the project** (including project summary, coordinator contact details, list of participants, European flag and funding statement and special logo and project results) on the beneficiaries' **websites** or **social media accounts**.

SPECIFIC RULES FOR CARRYING OUT THE ACTION (— ARTICLE 18)

Implementation in case of restrictions due to security or EU strategic autonomy

Where the call conditions restrict participation or control due to security or EU strategic autonomy reasons, the beneficiaries must ensure that none of the entities that participate as affiliated entities, associated partners, subcontractors or recipients of financial support to third parties are established in countries which are not eligible countries or target countries set out in the call conditions (or are controlled by such countries or entities from such countries) — unless otherwise agreed with the granting authority.

The beneficiaries must moreover ensure that any cooperation with entities established in countries which are not eligible countries or target countries set out in the call conditions (or are controlled by such countries or entities from such countries) does not affect the security interests or EU strategic autonomy and avoids potential negative effects over security of supply of inputs critical to the action.

Specific rules for PAC Grants for Procurement

When implementing innovative procurements in PAC Grants for Procurement, the beneficiaries must respect the following conditions:

- avoid any conflict of interest and comply with the principles of transparency, non-discrimination, equal treatment, sound financial management, proportionality and competition rules
- assign the ownership of the intellectual property rights under the contracts to the contractors (unless there are exceptional overriding public interests which are duly justified in Annex 1), with the right of the buyers to access results — on a royalty-free basis — for their own use and to grant (or to require the contractors to grant) non-exclusive licences to third parties to exploit the results for them — under fair and reasonable conditions — without any right to sub-license
- allow for all communications to be made in English (and any additional languages chosen by the beneficiaries)
- ensure that prior information notices, contract notices and contract award notices contain information on the EU funding and a disclaimer that the EU is not participating as contracting authority in the procurement
- allow for the award of multiple procurement contracts within the same procedure (multiple sourcing)
- for procurements involving classified information: apply the security rules set out in Annex 5 mutatis mutandis to the contractors and the background and results of the contracts

- where the call conditions restrict participation or control due to security or EU strategic autonomy reasons: apply the restrictions set out in Annex 5 mutatis mutandis to the contractors and the results under the contracts
- where the call conditions impose a place of performance obligation: ensure that the part of the activities that is subject to the place of performance obligation is performed in the eligible countries or target countries set out in the call conditions
- to ensure reciprocal level of market access: where the WTO Government Procurement Agreement (GPA) does not apply, ensure that the participation in tendering procedures is open on equal terms to bidders from EU Member States and all countries with which the EU has an agreement in the field of public procurement under the conditions laid down in that agreement, including all Horizon Europe associated countries. Where the WTO GPA applies, ensure that tendering procedures are also open to bidders from states that have ratified this agreement, under the conditions laid down therein.

Specific rules for Grants for Financial Support

When implementing financial support to third parties in Grants for Financial Support, the beneficiaries must respect the following conditions:

- avoid any conflict of interest and comply with the principles of transparency, non-discrimination and sound financial management
- for the selection procedure and criteria:
 - publish open calls widely (including on the Funding & Tenders Portal and the beneficiaries' websites)
 - keep open calls open for at least two months
 - inform recipients of call updates (if any) and the outcome of the call (list of selected projects, amounts and names of selected recipients)

Specific rules for JU actions

JU actions must contribute to the long-term implementation of the JU partnership, including the JU Strategic Research and Innovation Agenda, the JU objectives and the exploitation of research and innovation results.

Moreover, when implementing JU actions, the members and contributing partners of the Joint Undertaking must fulfil their obligations regarding contributions to the Joint Undertaking:

- the description of the action in Annex 1 must include, for beneficiaries, affiliated entities, associated partners or other participants or third parties which are members or contributing partners, the estimated contributions to the action, i.e.:
 - in-kind contributions to operational activities ('IKOP'; if applicable)
 - in-kind contributions to additional activities linked to the action ('IKAA'; if applicable)
 - financial contributions ('FC'; if applicable)

- the contributions must be reported during the implementation of the action in the Portal Continuous Reporting tool
- at the end of the action, the members and contributing partners that have not received funding under the grant must ensure that financial and in-kind contributions of EUR 430 000 or more (see Article 21) are supported by statements of contributions (CS) and certificates on the statements of contributions (CCS) which fulfil the following conditions:
 - be provided by a qualified approved external auditor which is independent and complies with Directive 2006/43/EC (or for public bodies: by a competent independent public officer)
 - the verification must be carried out according to the highest professional standards to ensure that the statements of contributions comply with the provisions under the Agreement and the applicable JU Regulation, that the contributions cover activities that are part of the action and that they have not been reimbursed by the grant
- contributions must comply with the following conditions:
 - costs covered by financial contributions cannot be claimed for reimbursement under the JU grant.

The beneficiaries must comply with the additional IPR, dissemination and exploitation obligations set out in the call conditions (Article 16 and Annex 5), in particular:

- for all JU grants: the granting authority right to object to transfers or licensing also applies to results generated by beneficiaries not having received funding under the grant.

In addition to the obligations set out in Article 17, communication and dissemination activities as well as infrastructure, equipment or major results funded under JU actions must moreover display the Joint Undertaking's special logo:



and the following text:

“The project is supported by the [insert JU name] and its members [*OPTION for actions with national contribution top-ups*: (including top-up funding by [name of the national funding authority])].”

For EuroHPC JU grants, the beneficiaries must respect the following conditions when implementing actions with national contribution top-ups from Participating States:

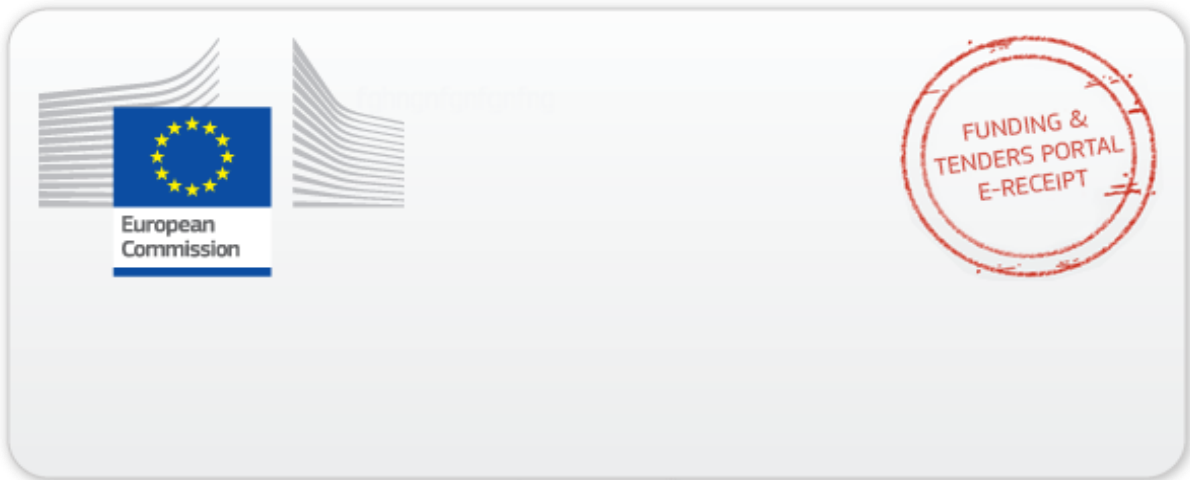
- the beneficiaries must ensure visibility of the national contributions (see below)

- the payment deadlines for prefinancing, interim or final payments are automatically suspended if a national funding authority is late with its payments to the Joint Undertaking for the national contribution top-up
- the European Anti-Fraud Office (OLAF), European Public Prosecutor's Office (EPPO), European Court of Auditors (ECA), the National Court of Auditors and other national authorities can exercise their control rights on the project implementation and costs declared, including for the national contribution top-up.

Specific rules for blending operations

When implementing blending operations, the beneficiaries acknowledge and accept that:

- the grant depends on the approved financing from the Implementing Partner and/or public or private investors for the project
- they must inform the granting authority both about the approval for financing and the financial close — within 15 days
- the payment deadline for the first prefinancing is automatically suspended until the granting authority is informed about the approval for financing
- both actions will be managed and monitored in parallel and in close coordination with the Implementing Partner, in particular:
 - all information, data and documents (including the due diligence by the Implementing Partner and the signed agreement) may be exchanged and may be relied on for the management of the other action (if needed)
 - issues in one action may impact the other (e.g. suspension or termination in one action may lead to suspension also of the other action; termination of the grant will normally suspend and exit from further financing and vice versa, etc.)
- the granting authority may disclose confidential information also to the Implementing Partner.



This electronic receipt is a digitally signed version of the document submitted by your organisation. Both the content of the document and a set of metadata have been digitally sealed.

This digital signature mechanism, using a public-private key pair mechanism, uniquely binds this eReceipt to the modules of the Funding & Tenders Portal of the European Commission, to the transaction for which it was generated and ensures its full integrity. Therefore a complete digitally signed trail of the transaction is available both for your organisation and for the issuer of the eReceipt.

Any attempt to modify the content will lead to a break of the integrity of the electronic signature, which can be verified at any time by clicking on the eReceipt validation symbol.

More info about eReceipts can be found in the FAQ page of the Funding & Tenders Portal.

<https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/faq>