AMENDMENT No AMD-101127940-2

Project: 101127940 — TEST-CERT-CZ

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

1 . Change of Annex 1

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

2 . Change of the project duration

The project duration in the **Data Sheet** is changed to 39.

3. Change of the reporting periods

The reporting period(s) in the **Data Sheet** are changed to:

- RP 1: month 1 to month 21
- RP 2: month 22 to month 39

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

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

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

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

SIGNATURES

For the coordinator

[redacted]

For the granting authority

[redacted]

Done in English

Enclosures: Grant Agreement Data Sheet
Grant Agreement Annex 1

ANNEX 1

Digital Europe Programme (DIGITAL)

Description of the action (DoA)

Part A

Part B

DESCRIPTION OF THE ACTION (PART A)

COVER PAGE

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

PROJECT *Grant Preparation (General Information screen) — Enter the info.*	
Project number:	101127940
Project name:	Building Testing and Certification Capabilities in the Czech Republic
Project acronym:	TEST-CERT-CZ
Call:	DIGITAL-ECCC-2022-CYBER-03
Topic:	DIGITAL-ECCC-2022-CYBER-03-TEST-CERT-CAPABILTIES
Type of action:	DIGITAL-JU-GFS
Service:	ECCC
Project starting date:	fixed date: 1 December 2023
Project duration:	39 months

TABLE OF CONTENTS

PROJECT SUMMARY

Project summary

Grant Preparation (General Information screen) — Provide an overall description of your project (including context and overall objectives, planned activities and main achievements, and expected results and impacts (on target groups, change procedures, capacities, innovation etc)). This summary should give readers a clear idea of what your project is about.

Use the project summary from your proposal.

The objective of this project is to increase and facilitate security and interoperability of testing capabilities and certification of connected ICT systems by cascade funding provided by the NCC-CZ. This aims to improve the capabilities and cooperation of cybersecurity certification stakeholders in line with the objectives of Regulation (EU) 2019/881 (“CSA”).

LIST OF PARTICIPANTS

PARTICIPANTS

Grant Preparation (Beneficiaries screen) — Enter the info.

Number	Role	Short name	Legal name	Country	PIC
1	COO	NCISA	NARODNI URAD PRO KYBERNETICKOU A INFORMACNI BEZPECNOST - NUKIB	CZ	907198418
1.1	AE	CSH	CYBERSECURITY HUB, ZU	CZ	889292509

LIST OF WORK PACKAGES

Work packages

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

Work Package No	Work Package name	Lead Beneficiary	Effort (Person-Months)	Start Month	End Month	Deliverables
WP1	Project Management and Coordination	1 - NCISA	23.00	1	39	D1.1 – Project Management Handbook D1.2 – Communication and Dissemination Plan D1.3 – Internal Project Progress Report 1 D1.4 – Internal Project Progress Report 2
WP2	Financial Support to Third Parties	1 - NCISA	49.00	1	39	D2.1 – FSTP Mechanism Documentation D2.2 – Strategic Agenda D2.3 – FSTP Call Documentation D2.4 – Supported Projects and Evaluation Report D2.5 – Activity and Communication Report D2.6 – Supported Projects and Evaluation Report II.

Work package WP1 – Project Management and Coordination

Work Package Number	WP1	Lead Beneficiary	1 - NCISA
Work Package Name	Project Management and Coordination		
Start Month	1	End Month	39

Objectives
▪ Manage the project and coordinate the activities taking into account personnel, budget and time during the three-year duration of the project (financial and grant management) and monitor the progress (disbursement of funds, meeting objectives). ▪ Ensure project team and consortium partners coordination (division of work, regular meetings). ▪ Communication and reporting with the grant authority/EC.

Description
The goal of this WP is to manage the project and coordinate the activities taking into account personnel, budget and time during the three-year duration of the project and monitor the progress (disbursement of funds, meeting objectives). The following tasks are envisioned: - T1.1 Project management: Overseeing the implementation of the project and its activities (meeting objectives, deliverables) and the project budget (reimbursement of funds, expenditures) - T1.2 Project team coordination: Ensure the project team coordination (division of work and regular meetings to assess the progress of the project and address potential needs), coordination of consortium partners (GA meetings) - T1.3 EC reporting: Preparing and submitting reports on the progress of the project to the grant authority

Work package WP2 – Financial Support to Third Parties

Work Package Number	WP2	Lead Beneficiary	1 - NCISA
Work Package Name	Financial Support to Third Parties		
Start Month	1	End Month	39

Objectives
▪ Set up a financial support program for third parties (FSTP) with the aim of supporting the uptake and dissemination of state-of-the-art cybersecurity solutions by SMEs and other entities.

Description
The objective of WP2 is to set up a financial support program for third parties (FSTP) during the project period, with the aim of supporting the uptake and dissemination of state-of-the-art cybersecurity solutions by SMEs and other entities. The following tasks are planned: - T2.1 Setting up and adjusting the NCC-CZ FSTP mechanism – Making adjustments to the NCC-CZ FSTP mechanism if necessary. - T2.2 Preparation of the Strategic Agenda – Identification of the topics to be supported (consulting with relevant entities and taking into account the state of the art and the specific needs of the Czech Republic). - T2.3 Identification of the pool of expert evaluators – Identify the requirements for evaluators of the project proposals. - T2.4 Preparation of the open calls and calls activation – Preparation of the Call documentation and activation of the open calls. - T2.5 Dissemination of information regarding the FSTP calls and information support – Informing the relevant stakeholders about the funding opportunities and the upcoming calls, providing information support for the applicants. - T2.6 Evaluation of proposals and selection of successful proposals – Evaluation of the project proposals in cooperation with the NCC-CZ Council and expert evaluators, selection of successful projects. - T2.7 Grant agreement preparation – Prepare the grant agreements with successful applicants for support.

- T2.8 Monitoring of the supported projects, final evaluation and presentation of the project outcomes – Monitor and oversee the supported projects (objectives, progress, grant agreements conditions). Evaluate the project after its end and help disseminate the project outcomes.

The goal is to provide FSTP (preferably in the form of lump sum) to support building testing and certification capabilities in the Czech Republic. It is envisioned to launch calls to cover even the upcoming cybersecurity certification schemes, aiming at activities in line with the spirit and objectives of the proposed amendment of CSA, and to provide financial support to an even wider group of entities, including, to the degree possible and sensible, entities from other eligible European countries and consortia of eligible European entities. Therefore, more calls may be launched in the duration of the project taking into account the current situation at the national and EU level.

To further motivate the potential applicants for financial support, we plan to organize a FSTP/Certification workshop to pass on relevant information regarding the details of the upcoming calls and the application process, as well as provide information in the area of cybersecurity certification. We also plan to organize a final event where the outcomes of the supported projects will be presented. During the project implementation, there will be also other communication activities in line with the KPIs and Communication and Dissemination Strategy, for example newsletters and website updates.

The first few months are dedicated to the identification and preparation of the open calls and the set-up of the FSTP mechanism of the NCC-CZ, which is a part of the project proposal submitted in the call Deploying The Network Of National Coordination Centres With Member States. Therefore, the FSTP mechanism prepared for the functioning of the NCC-CZ will be used, with adjustments, if necessary, in this project. The timetable is set in a way that allows to launch calls and other activities during the reserved time period, it is not envisioned for the activities to be completed at the end of the reserved time in all cases.
Conditions for implementing FSTP grants:

▪ Max amount per third party: 100 000 EUR with 50 % co-financing by the third party
▪ Criterium for calculating the exact amount: inclusion of all costs (personnel, travel, equipment, other)
▪ Types of activity: Capacity building including for thread-based penetration testing; e.g. for the acquisition of certification testbeds; exchange of best practices and staff trainings; deploy innovative evaluation methods for specific ICT products or components; innovative evaluation methods implemented by accreditation body, support standardisation actions; Testing and certifying ICT products, ICT services or ICT process; Auditing infrastructures in term of cybersecurity resilience; Standardization actions (e.g., creation of protection profiles or adoption/improvement of standards used in certification schemes), considering activities by European and international standardisation organisations as appropriate; Cyber-security and interoperability testing capabilities on 5G disaggregated and open solutions.
▪Persons/categories of persons to be supported: (future) Conformity assessment bodies; Accreditation body; SMEs (manufacturers/providers, ICT equipment users).
▪Criteria and procedures for giving support: Relevance to EU and national cyber-security policy; Outcomes and deliverables; Strengthen conformity assessment bodies and accreditation body; Improve the cybersecurity and interoperability testing capabilities, including in the area of 5G disaggregated and open solutions and trusted chips; Support SMEs to audit their infrastructure in view of improving their cybersecurity protection; Support actions in the area of standardisation.
▪KPIs to measure outcomes and deliverables: Number of supported certification testbeds set up and innovative evaluation/assessment methods deployed for specific ICT products or components implemented by conformity assessment bodies or accreditation body; Additional certification and testing services provided by a beneficiary as a result of the activities; Standardisation actions with European and international standardisation organisations that were supported, e.g. number or novelty of standards and specifications published in reference to evaluation tools and methods utilised by a beneficiary; Knowledge and capacity building activities e.g., exchange of best practices, staff trainings; Increase in the number or expansion of scope of ICT products, services or processes of SMEs that received support for their testing and certification; ICT equipment's audits in terms of cybersecurity resilience by SMEs which were supported; Cybersecurity and interoperability testing capabilities supported on 5G disaggregated and open solutions or on chips.
▪Impact of the project: improvement of the cyber resilience of the Czech Republic and/or EU
▪Potential/opportunities for implementation of the project outputs
▪Quality and maturity of the project proposal
▪Alignment with the objectives of the call
▪Soundness of the implementation plan and efficient use of resources
▪Capacity of the applicants to carry out the proposed work

This work package will be implemented in the form of several open calls targeted at defined specific goals and forms.

The planned implementation mechanism is inspired by conditions of the Digital Europe Programme, e.g., in terms of main evaluation criteria (relevance, implementation, impact) or eligible costs definition and reporting mechanisms.

The grants will be administered taking into account the following conditions as listed in the Call document:

1. the calls must be open, published widely and conform to EU standards concerning transparency, equal treatment, conflict of interest and confidentiality
2. the calls must be published on the Funding & Tenders Portal, and on the participants' websites
3. the calls must remain open for at least two months
4. if call deadlines are changed this must immediately be published on the Portal and all registered applicants must be informed of the change
5. the outcome of the call must be published on the participants' websites, including a description of the selected projects, award dates, project durations, and final recipient legal names and countries
6. the calls must have a clear European dimension.

STAFF EFFORT

Staff effort per participant

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

Participant	WP1	WP2	Total Person-Months
1 - NCISA	17.00	34.00	51.00
1.1 - CSH	6.00	15.00	21.00
Total Person-Months	23.00	49.00	72.00

LIST OF DELIVERABLES

Deliverables

Grant Preparation (Deliverables screen) — Enter the info.

The labels used mean:

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

Deliverable No	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month)
D1.1	Project Management Handbook	WP1	1 - NCISA	R — Document, report	SEN - Sensitive	3
D1.2	Communication and Dissemination Plan	WP1	1.1 - CSH	R — Document, report	SEN - Sensitive	3
D1.3	Internal Project Progress Report 1	WP1	1 - NCISA	R — Document, report	SEN - Sensitive	9
D1.4	Internal Project Progress Report 2	WP1	1 - NCISA	R — Document, report	SEN - Sensitive	27
D2.1	FSTP Mechanism Documentation	WP2	1.1 - CSH	R — Document, report	SEN - Sensitive	9
D2.2	Strategic Agenda	WP2	1 - NCISA	R — Document, report	PU - Public	9
D2.3	FSTP Call Documentation	WP2	1 - NCISA	R — Document, report	PU - Public	16
D2.4	Supported Projects and Evaluation Report	WP2	1 - NCISA	R — Document, report	SEN - Sensitive	21
D2.5	Activity and Communication Report	WP2	1 - NCISA	R — Document, report	PU - Public	39
D2.6	Supported Projects and Evaluation Report II.	WP2	1 - NCISA	R — Document, report	SEN - Sensitive	28

Deliverable D1.1 – Project Management Handbook

Deliverable Number	D1.1	**Lead Beneficiary**	1 - NCISA
Deliverable Name	Project Management Handbook		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	3	**Work Package No**	WP1

Description
The Project Management Handbook streamlines the project's initiation through consolidation of activities, representing a core document providing essential information about project management in terms of administration, procedures, communication, knowledge management, monitoring etc. It will contain objectives, responsibilities, and communication workflow. The document will be in English and Electronic.

Deliverable D1.2 – Communication and Dissemination Plan

Deliverable Number	D1.2	**Lead Beneficiary**	1.1 - CSH
Deliverable Name	Communication and Dissemination Plan		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	3	**Work Package No**	WP1

Description
Communication and Dissemination Strategy will identify the main communication channels for the distribution of information to the community and target groups, design an appropriate information strategy to maximize the reach of the project and its outputs. The strategy will then be implemented in the individual project activities. It will also cover the exploitation. The document will be in English and Electronic.

Deliverable D1.3 – Internal Project Progress Report 1

Deliverable Number	D1.3	**Lead Beneficiary**	1 - NCISA
Deliverable Name	Internal Project Progress Report 1		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	9	**Work Package No**	WP1

Description
Internal project report to describe the progress regarding the implementation of the project. The report will be Electronic and in English.

Deliverable D1.4 – Internal Project Progress Report 2

Deliverable Number	D1.4	**Lead Beneficiary**	1 - NCISA
Deliverable Name	Internal Project Progress Report 2		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	27	**Work Package No**	WP1

Description
Internal project report to describe the progress regarding the implementation of the project. The report will be Electronic and in English.

Deliverable D2.1 – FSTP Mechanism Documentation

Deliverable Number	D2.1	**Lead Beneficiary**	1.1 - CSH
Deliverable Name	FSTP Mechanism Documentation		
Type	R — Document, report	**Dissemination Level**	SEN - Sensitive
Due Date (month)	9	**Work Package No**	WP2

Description
FSTP mechanism documentation will include feasibility study proposing mechanism for project selection and monitoring and will be amended by supporting toolkit (NCC council procedural rules, sample project calls, application forms, evaluation forms, sample grant agreements, etc.). The document will be Electronic and in English.

Deliverable D2.2 – Strategic Agenda

Deliverable Number	D2.2	**Lead Beneficiary**	1 - NCISA
Deliverable Name	Strategic Agenda		
Type	R — Document, report	**Dissemination Level**	PU - Public
Due Date (month)	9	**Work Package No**	WP2

Description
The Strategic Agenda will identify the topics to be supported, consulting with relevant entities and taking into account the state of the art and the specific needs of the Czech Republic). The Agenda will be Electronic and in English.

Deliverable D2.3 – FSTP Call Documentation

Deliverable Number	D2.3	**Lead Beneficiary**	1 - NCISA
Deliverable Name	FSTP Call Documentation		
Type	R — Document, report	**Dissemination Level**	PU - Public
Due Date (month)	16	**Work Package No**	WP2

Description
FSTP Call documentation will include full and final version of the FSTP call and amendments including rules of procedure, sample agreements, application form, etc. The documentation will be Electronic and in English.

Deliverable D2.4 – Supported Projects and Evaluation Report

Deliverable Number	D2.4	**Lead Beneficiary**	1 - NCISA
Deliverable Name	Supported Projects and Evaluation Report		

Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	21	Work Package No	WP2

Description
This report will include a list of supported project and description of their expected impact and will be amended by the evaluation forms and NCC council meeting minutes. The Report will be Electronic and in English.

Deliverable D2.5 – Activity and Communication Report

Deliverable Number	D2.5	Lead Beneficiary	1 - NCISA
Deliverable Name	Activity and Communication Report		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	39	Work Package No	WP2

Description
Information regarding the communication and dissemination activities of the project together with the information regarding the planned workshops/events will be subject to the EU mandatory periodic reports (in M18 and M36) and other project progress reports and updates (in M9 and M27).

Deliverable D2.6 – Supported Projects and Evaluation Report II.

Deliverable Number	D2.6	Lead Beneficiary	1 - NCISA
Deliverable Name	Supported Projects and Evaluation Report II.		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	28	Work Package No	WP2

Description
This report will include a list of supported project (projects included in the II. Call) and description of their expected impact and will be amended by the evaluation forms and NCC council meeting minutes. The Report will be Electronic and in English.

LIST OF MILESTONES

Milestones

Grant Preparation (Milestones screen) — Enter the info.

Milestone No	Milestone Name	Work Package No	Lead Beneficiary	Means of Verification	Due Date (month)
1	Mid-term project review	WP1	1 - NCISA	Mid-term project assessment report (included in the mandatory EU report).	18
2	Final project review and project closure	WP1	1 - NCISA	Final project assessment report (included in the mandatory EU report).	36
3	FSTP Calls Activation	WP2	1 - NCISA	Launch of the calls on the F&T Opportunities Portal. This milestone is connected to the deliverable called "FSTP Call documentation".	16
4	Projects closure and evaluation	WP2	1 - NCISA	Final report and evaluation of the supported projects will be a part of the final mandatory EU report.	39

LIST OF CRITICAL RISKS

Critical risks & risk management strategy

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

Risk number	Description	Work Package No(s)	Proposed Mitigation Measures
1	Communication problems between the project partners can cause delays to the implementation of the project.	WP2, WP1	Kick-off meeting will be held to establish personal contacts; the Project Management Handbook will set procedures for the day-to-day management administration and communication, operational management.

Critical risks & risk management strategy

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

Risk number	Description	Work Package No(s)	Proposed Mitigation Measures
2	Withdrawal of a team member during the project implementation.	WP2, WP1	It will be ensured that the project team is transparent and robust, uses methods of substitutability and horizontal information sharing and that the conditions are set up in a motivational and long-term way.
3	A partner will fail to fulfil an obligation or leave the project altogether.	WP2, WP1	The selection of consortium members is based on already existing strategic cooperation within other projects and activities. Regular monitoring of the external conditions will be conducted with eventual reactions to the changes.
4	Financial shortage due to costs increase by inflation and/or by CZK currency ratio fluctuations.	WP2, WP1	Realistic planning of the cost setting and spending backed by the Consortium agreement and through financial coordination will be ensured.
5	Failure to observe the proposed project timetable.	WP2, WP1	Regularly consulting the timetable, setting up control mechanisms, realistic project planning (providing enough time and resources), highly experienced team.
6	Slow uptake of the FSTP process.	WP2	Early communication with the target audience about the upcoming calls will be ensured, together with cooperation with partners and national stakeholders to pass on information regarding the funding opportunities and provide support.
7	Delays in establishing the certification schemes (entities will not apply for funding if they will not have enough information, NCC will not have enough information to launch the FSTP calls).	WP2	In order to mitigate the risks, active participation in meetings concerning the scheme preparation, ECCG meetings and active approach in the Committee meetings will be ensured.
8	Low interest in the open calls.	WP2	Mapping the needs and capacities of the targeted stakeholders. In this context, pre-mapping of interest was done before the submission of the project application, the mapping will continue during the project implementation to be in line with the capacities. Also, the funding opportunities will be actively presented and advertised targeting the relevant audience sufficiently in advance.
9	All interested parties are focusing on the same topic.	WP2	Identification of areas/topics that are attractive for the targeted stakeholders. Pre-mapping of the interest among the targeted stakeholders, identification of topics in line with the interest and needs of the targeted audience and the CZ.

PROJECT REVIEWS

Project Reviews

Grant Preparation (Reviews screen) — Enter the info.

Review No	Timing (month)	Location	Comments
RV1	18	To be determined	
RV2	36	To be determined	

Digital Europe Programme (DIGITAL)

Description of the action (DoA)

Part B

Version 1.0
01 November 2021

DESCRIPTION OF THE ACTION (PART B)

HISTORY OF CHANGES		
DATE	PAGE/SECTION	NATURE OF CHANGE AND REASON
31.5.2023	Critical risks	Two risks connected to the WP2: Financial Support to Third Parties were added (Low interest in the open calls; All interested parties are focusing on the same topic) based on the received recommendations.
31.5.2023	WP1: Project Management and Coordination (Deliverables)	The dissemination level was changed in “Project Management Handbook” and “Communication and Dissemination Plan” from public to sensitive due to the possibly sensitive nature of the information.
31.5.2023	WP1: Project Management and Coordination	The dissemination level of the deliverable “Internal Project Progress Report 1” and “Internal Project Progress Report 2” was changed from public to sensitive due to possibly sensitive nature of the information regarding the progress of the project implementation.
2.6.2023	WP1: Project Management and Coordination	Deliverable “EC Periodic Reports” was deleted since the reporting towards EU is already covered separately.
2.6.2023	WP1: Project Management and Coordination and WP2: Financial Support to Third Parties	The language of deliverables was changed to English due to the expected reviews. The documents may also exist in Czech language; however, convenience translations will be used for submitting the deliverables.
2.6.2023	WP1: Project Management and Coordination and Dissemination and communication of the project and its results	A sentence “*It will also cover the exploitation*.” was added to the description of the deliverable “Communication and Dissemination Plan” based on a recommendation. The same sentence was also added to the description of Communication and Dissemination Plan to be in line with the specific topic conditions regarding an additional deliverable on dissemination and exploitation, to be submitted in the first six months of the project.
27.6.2023	WP1: Project Management and Coordination	The description of the planned milestones, the M1 (“Mid-term project review”) and M2 (“Final project review and project closure”) was updated with “*included in the mandatory EU report*" to link the means of verification of these milestones to the mandatory EU reporting and explain that there will not be double documents concerning the same topic.
27.6.2023	WP2: Financial Support to Third Parties	A milestone description of M3 “FSTP Calls Activation” was updated with “*This milestone is connected to the deliverable called "FSTP Call documentation.*”
27.6.2023	WP2: Financial Support to Third Parties	A milestone description of M4 (“Projects closure and evaluation”) was updated with “*will be a part of the final mandatory EU report*”.
27.6.2023	WP2: Financial Support to Third Parties	Deliverable called “Final Report” was deleted since the topic (final report and evaluation regarding the supported projects) will be finally covered in the mandatory EU report at the end of the project and in Milestone 4.
27.6.2023	WP2: Financial Support to Third Parties	The deliverables “FSTP/Certification Workshop for targeted stakeholders” and “Closing event” were deleted and instead a new deliverable “Activity and Communication Report” was created together with this description “*Information regarding the communication and dissemination activities of the project together with the information regarding the planned workshops/events will be subject to the EU mandatory periodic reports (in M18 and M36) and other project progress report and updates (in M9 and M27).”*
27.6.2023	WP1: Project Management and Coordination	Deliverable “Internal Project Progress Reports” to be submitted in month 6, 12, 18, 24, 30 and 36 was divided between 2 deliverables “Internal project Progress Report 1” and “Internal project Progress Report 2” and updated with the description *“Internal project report to describe the progress regarding*

		the implementation of the project. The report will be Electronic and in English." The reporting was reduced since it is partly already covered by the mandatory EU reporting.
29.6.2023	1.1 Objectives and Activities	Based on the received recommendations, the objectives of the project were linked to the KPIs that are described in more detail in section 3. Also, the description of the "Objectives and activities" was updated to include the possibility to support entities from other eligible European countries to the degree possible and sensible, and to explain that the financial support might also concentrate on activities in line with the spirit and objectives of the proposed amendment of the CSA.
30.6.2023	3.1 Expected outcomes and deliverables – Dissemination and communication	Based on the received recommendations, the values of the set KPIs were elaborated (however, it is highly dependent on the interest of the third parties) and additional KPIs were provided (such as number of expected projects and communication activities).
30.6.2023	Competitiveness and benefits for the society	A sentence "*However, we understand, that developing and enhancing the testing and certification capabilities and capacities in the Czech Republic contributes to the effort for building a common European system of cybersecurity certifications, therefore we expect entities from other eligible European countries to the degree possible and sensible, to benefit from NCC-CZ calls. Also, our actions will be coordinated with other NCCs to exchange best practices, avoid overlapping capacities, contribute to the common goal and have a greater outreach at EU level."* was added to highlight the European cooperation with other NCCs in connection to developing and enhancing the testing and certification capabilities and capacities in the Czech Republic and the possible involvement of other European entities, based on the provided recommendations.
30.6.2023	WP2: Financial Support to Third Parties	The description of the WP2 was updated to include, in line with previous textual edits, the possibility to provide funding to entities from eligible European countries and consortia of eligible European entities (to the level possible and sensible) as well as the possibility to aim at activities in line with the spirit and objectives of the proposed amendment of CSA. The planned communication activities were also elaborated a bit more, adding to the planned FSTP/Certification workshop information regarding the Final event ("*We also plan to organize a final event where the outcomes of the supported projects will be presented*") and newsletters, website updates and other activities in line with the Communication and Dissemination Strategy. In the "types of activity" part, the text was updated with "*innovative evaluation methods implemented by accreditation body*" and finally, in the "KPIs to measure outcomes and deliverables" this point was added "*innovative evaluation/assessment methods implemented by conformity assessment bodies or accreditation body"* to be in line.
30.6.2023	WP2: Financial Support to Third Parties	The dissemination level of the deliverable "*Supported projects and evaluation report*" was changed from public to sensitive due to a possibly sensitive nature of the document.
20.5.2025	1.1 Objectives and activities	Objective *"Help enhance cybersecurity and interoperability testing abilities for 5G decentralized and open solutions*" was removed due to a change in the focus of the project (and unfinished certification scheme). Activities from "*Providing financial support to help CABs invest in necessary infrastructure, tools, and personnel for CRA-compliant certification processes*" to *"Supporting standardization efforts by contributing to the development of protection profiles and improving certification frameworks in coordination with European and international bodies*." and a sentence "*These efforts will ensure that CABs and laboratories can effectively assess ICT products and services under the CRA, ultimately strengthening cybersecurity resilience and trust in certification processes across the European market*." were added.

20.5.2025	1.2 Contribution to long-term policy objectives, policies and strategies — Synergies	Added four paragraphs concerning CRA as follows *"Furthermore, the project complements existing national efforts by ensuring that CABs and SMEs receive targeted financial and technical support to accelerate their readiness for CRA-compliant certification. While NCISA's Development Framework outlines the vision for a robust certification ecosystem, this initiative translates those strategic goals into concrete actions by equipping stakeholders with the necessary expertise, infrastructure, and assessment methods. This is particularly needed because the CRA regulation is mandatory, and SMEs will not be able to avoid it.* *By integrating these activities with broader EU frameworks, including the NIS2 Directive and Cyber Resilience Act, the project fosters cross-border cooperation and enhances the interoperability of certification processes. This will not only strengthen the Czech Republic's position within the European cybersecurity certification landscape but also contribute to the harmonization of cybersecurity requirements across the Single Market, reinforcing the overall resilience of the digital economy.* *In addition to supporting conformity assessment and certification activities under the Cyber Resilience Act (CRA), the project may also focus on enabling the development of targeted support services for entities performing self-assessments. These services could include the creation of standardized templates, technical tools for structured evaluation, or consulting capacities tailored to help organizations meet the essential requirements set by the CRA. Although such activities do not fall under formal certification, they contribute to the broader objectives of standardization, capacity-building, and market preparedness, and thus align with the overall scope of the call.* *Furthermore, the project aims to create synergies that extend beyond the immediate implementation horizon. By supporting the development of relevant technical and organizational capacities, the initiative will help lay the groundwork for the future expansion of services—especially toward formal certification in forthcoming EU schemes. Participating entities will gain experience with compliance processes, accreditation pathways, and staff qualification, making them better positioned to meet future regulatory demands and offer trusted cybersecurity assurance services on the European market."*
20.5.2025	3.1 Expected outcomes and deliverables — Dissemination and communication	Following KPIs were removed: • 3 Supported certification testbeds established, and innovative evaluation/assessment methods implemented by conformity assessment bodies or accreditation body, • 3 Certification and testing services provided by the beneficiaries as a result of the initiatives, • 1 Standardization actions supported with European and international standardization organizations, e.g., quantity and originality of standards and specifications published in regards to evaluation tools and methods used by beneficiaries • Increase in the number or extent of ICT products, services or processes of SMEs that received support for testing and certification by 2, • 2 Cybersecurity resilience audits of ICT equipment by supported SMEs, • 1 Cybersecurity and interoperability testing capabilities supported on 5G disaggregated and open solutions or on chips. • The following KPIs have been added: • At least 1 Certification body (CABs) financially supported to prepare for CRA requirements • 2 SMEs supported in preparing for CRA certification • At least 1 training platform focused on CRA capacity building

		• Development or implementation of at least 1 supportive service or tool facilitating self-assessment in alignment with the CRA framework (e.g., specialized consultancy service, template documentation, or a technical self-assessment tool). • At least 4 Guidance or methodical documents created or updated by third party (public awereness materials) in alignment with CRA implementation • 1 Collaborative initiative launched
20.5.2025	2.3 Capacity to carry out the proposed work	The project teams and staff table has been updated.
6.6.2025	DoA part A - Reporting periods	After consultation with the project officer, the first reporting period was extended to 21 months.
14.7.2025	DoA Part B - Timetable	Another quarter has been added for the fourth year of the project implementation and the implementation of tasks 2.4, 2.5, and 2.6 has been extended by one quarter.
14.7.2025	DoA Part A - Deliverables	The submission of D9 "Activity and Communication Report" has been postponed from 36 to 39 months.
14.7.2025	DoA Part A - Milestone Description	Milestone No. 4 Projects closure and evaluation - delivery date postponed to month 39.
14.7.2025	DoA part A - Work Package Description	The implementation period for both work packages has been extended to 39 months.

TABLE OF CONTENTS

#@APP-FORM-DEP@#
#@PRJ-SUM-PS@# [This document is tagged. Do not delete the tags; they are needed for the processing.]

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?

The objective of this project is to increase and facilitate security and interoperability of testing capabilities and certification of connected ICT systems by cascade funding provided by the NCC-CZ. This aims to improve the capabilities and cooperation of cybersecurity certification stakeholders in line with the objectives of Regulation (EU) 2019/881 ("CSA").

The Czech Republic is a member of the international agreement facilitating the mutual recognition of Common Criteria (CCRA) as a certificate consuming member, but not as a certificate issuer. This consequentially implies that Czech Republic does not have the necessary infrastructure or personnel capacities to issue certificates or provide testing facilities for Common Criteria. However, there is significant potential for growth and improvement in field of cybersecurity certification.

Czech Republic has state-of-the-art laboratories that are dedicated to providing services for Industrial and Automation Control Systems (IACS) or Internet of Things. Additionally, the national accreditation body is equipped with the capabilities to offer accreditation for Information Security Management System, Information Technology Services Management System, or Business Continuity Management System.

Despite its limited experience in cybersecurity certification, Czech Republic is determined to make progress in this crucial field. The Czech National Cyber and Information Security Agency (NCISA) serves as the central administrative body for cybersecurity including the role of NCCA (National Cyber Certification Authority), which implies that it oversees the implementation and monitoring of all CSA related obligations. Furthermore, NCISA is responsible for the protection of classified information, communication systems and cryptographic protection. Together in cooperation with its partner the CyberSecurity Hub (CSH), NCISA operates as the NCC-CZ, through which it plans to provide funding to stakeholders in the area of cybersecurity certification. The objective is to support the development and expansion of the country's cybersecurity certification infrastructure and expertise, including, to the degree possible and sensible, entities from other eligible European countries.
This project aims to provide following:

- Enhance the capacities of conformity assessment bodies and accreditation bodies, including thread-based penetration testing. This will include acquiring certification testbeds, exchanging best practices, providing staff training, utilizing innovative evaluation methods for specific ICT products or components, and supporting standardization efforts (such as creating protection profiles or improving standards used in certification schemes),
- Support small and medium-sized enterprises (SMEs) in testing and obtaining certification for the ICT products, services, or processes they offer, with priority given to proposals that demonstrate a positive impact on sectors affected by the COVID-19 pandemic (e.g., health sector),
- Support SMEs using ICT equipment to assess the cybersecurity resilience of their infrastructure by means of audit,
- Provide support for standardization efforts, actively participate in EU certification initiatives, including contributing to the development of protection profiles and supporting the refinement of standards used in European certification schemes,
- Enhance the capacities of conformity assessment bodies (CABs) by providing financial support, training, and resources for CRA-compliant certification processes. Expected outcomes and deliverables in the form of KPIs are more detailed in section 3. Impact, clause 3.1.

Support will concentrate on certification schemes specified in the Cybersecurity Act when appropriate and may also be offered for technical field not currently addressed by the schemes under the CSA, including activities in line with the spirit and objectives of the proposed amendment of CSA.
The contribution of this project to the overall Digital Europe Programme (DEP) is to:

- Build knowledge, capacity and skills related to cybersecurity certifications as well as best practices,
- Enhance resilience, elevate risk awareness, and attain basic levels of cybersecurity,
- Advance cybersecurity equipment, tools and data infrastructure

- Improve coordination among relevant stakeholders (National Accreditation Body (NAB), Conformity Assessment Body (CAB), ICT manufactures/providers and ICT users).

Enhancing the capacities of conformity assessment bodies (CABs) and accreditation bodies by:

- Providing financial support to help CABs invest in necessary infrastructure, tools, and personnel for CRA-compliant certification processes.
- Delivering specialized training programs to build expertise in CRA-related evaluation methods, security assessments, and risk management.
- Fostering collaboration between stakeholders such as national accreditation bodies, regulatory authorities, SMEs, and standardization organizations to ensure alignment with CRA requirements.
- Supporting standardization efforts by contributing to the development of protection profiles and improving certification frameworks in coordination with European and international bodies.

These efforts will ensure that CABs and laboratories can effectively assess ICT products and services under the CRA, ultimately strengthening cybersecurity resilience and trust in certification processes across the European market.

#@COM-PLE-CP@#

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.

Improvement and strengthening of testing capabilities and certification under the objectives of Cybersecurity Act is crucial for achieving a complex ecosystem where multiple stakeholders could get involved in the certification process. The development of appropriate certification capacities and capabilities together with the support of private sector is envisioned in the Action Plan for the National Cybersecurity Strategy of the Czech Republic 2021 – 2025 published by NCISA. According to the Action Plan, NCISA is responsible for fulfilling tasks and objectives stipulated by the Cybersecurity Act. Moreover, the Development Framework of NCISA from 2020 also considers the development of Czech framework of CABs as well as enhancing their capabilities. With the current situation and no other released european cybersecurity certification scheme, we are aiming to have a network of CABs by 2030 - primary focused on CRA, than we can focus again on CSA.

Czech Republic still considers using the future certification scheme for cloud service providers as a presumption of conformity in the context of the national cloud regulation, but it depends on the EU and finished work on EUCS.

The national activities and strategies are in line with the EU activities in the certification area, especially with the Cybersecurity Act, NIS2 Directive (Article 24) and Cyber Resilience Act (presumption of conformity with the proposed Regulation).

The project that we are proposing contributes significantly to the long-term policy objectives of the call's domain/area by providing SMEs with the resources and support they need to build their security auditing practices. This aligns with the relevant policies and strategies at both European and national levels, which prioritize the development and growth of SMEs as key drivers of economic growth and stability. The national accreditation body will also act as a recipient of the funds, using them to build their personal capacities and acquire necessary tools for delivering services in line with CSA.

Furthermore, the project complements existing national efforts by ensuring that CABs and SMEs receive targeted financial and technical support to accelerate their readiness for CRA-compliant certification. While NCISA's Development Framework outlines the vision for a robust certification ecosystem, this initiative translates those strategic goals into concrete actions by equipping stakeholders with the

necessary expertise, infrastructure, and assessment methods. This is particularly needed because the CRA is mandatory, and SMEs will not be able to avoid it.

By integrating these activities with broader EU frameworks, including the NIS2 Directive and Cyber Resilience Act, the project fosters cross-border cooperation and enhances the interoperability of certification processes. This will not only strengthen the Czech Republic's position within the European cybersecurity certification landscape but also contribute to the harmonization of cybersecurity requirements across the Single Market, reinforcing the overall resilience of the digital economy.

In addition to supporting conformity assessment and certification activities under the Cyber Resilience Act, the project may also focus on enabling the development of targeted support services for entities performing self-assessments. These services could include the creation of standardized templates, technical tools for structured evaluation, or consulting capacities tailored to help organizations meet the essential requirements set by the CRA. Although such activities do not fall under formal certification, they contribute to the broader objectives of standardization, capacity-building, and market preparedness, and thus align with the overall scope of the call.

Furthermore, the project aims to create synergies that extend beyond the immediate implementation horizon. By supporting the development of relevant technical and organizational capacities, the initiative will help lay the groundwork for the future expansion of services - especially toward formal certification in forthcoming EU schemes. Participating entities will gain experience with compliance processes, accreditation pathways, and staff qualification, making them better positioned to meet future regulatory demands and offer trusted cybersecurity assurance services on the European market.

#§COM-PLE-CP§#

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.*

The support and the development of Czech certification bodies will help to reinforce and secure the digital supply chain of the EU in several ways. Firstly, Czech bodies do have the local expertise in the Czech market and economy, which can help to identify and mitigate risks specific to the region. The development and support of Czech conformity assessment bodies can increase competition within the EU certification market, which can help to drive innovation and improve the overall quality of the certification process. Furthermore, it will improve accessibility of the certifications by allowing Czech as well as foreign companies to get their products and services certified for a reasonable cost, which is particularly important for SMEs that may be short of resources. Companies will thus not have to engage in certification process outside of the Czech Republic which would allow them to save on costs.

Moreover, by developing and enhancing the testing and certification capabilities and capacities in the Czech Republic, the industry will be able to engage in certification processes early on and benefit from the schemes with a view of compliance with the relevant EU policy measures aiming at improving the digital supply chain in the EU, such as the EU Cloud Certification Scheme. Conformity assessment bodies with appropriate capacities and capabilities are thus essential for the private sector to be able to comply with the cybersecurity policy measures that ensure an appropriate cybersecurity level of the certified products.

Although certification alone does not guarantee that a certified product would not be compromised, it improves the cybersecurity ecosystem and the security of the digital technology supply chain on both national and EU level. Certification of products thus guarantee that the products have certain level of security, making it harder for threat actors to engage in malicious activity. For that, it is vital to develop and improve the certification processes as well as conformity assessment bodies so that they can thoroughly test the products and evaluates their compliance with relevant cybersecurity certification schemes.

The development and support of the national certification bodies can play a key role in reinforcing and securing the digital supply chain of the EU. By providing local expertise, increasing competition, improving accessibility, increasing trust, and better protecting critical assets within the Czech Republic as well as in other EU member states, the certification bodies can contribute to building a more secure and resilient digital supply chain across the EU.

The project that we are proposing would significantly reinforce and secure the digital technology supply chain in the EU by supporting the development of robust security auditing practices among SMEs. SMEs are an important part of the digital technology supply chain, and the security of their products and services is essential to maintaining the overall security and stability of the EU's digital infrastructure.

The national accreditation body is an essential player in both securing the digital supply chain and providing services in regards to the EU cybersecurity certification ecosystem. This alone helps to maintain the integrity and reliability of the certification process, contributing to the overall security and stability of the digital technology supply chain in the EU.

1.4 Financial obstacles

Financial obstacles

Describe to what extent the project can overcome financial obstacles such as the lack of market finance.

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

Not applicable as stated in the Call document DIGITAL-ECCC-2022-CYBER-03.

#§PRJ-OBJ-PO§# #§REL-EVA-RE§# #@QUA-LIT-QL@# #@MAT-URI-MU@#

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.

In December 2021, NCISA received the authorization by the Czech government to ask for a nomination from the EU and request a capacity assessment for the NCC-CZ. At the same time, cooperation was established with the partner institution CyberSecurity Hub (CSH) by signing a memorandum of cooperation. Since then, NCISA and CSH have started discussing how to fulfil the tasks of the NCC-CZ with regard to the provision of financial support to third parties (FSTP) using the cascade funding mechanism. NCC-CZ has already received the positive result of the capacity assessment, therefore is now focusing on setting up mechanisms to ensure its ability to redistribute EU funds to entities.

Representatives from NCISA and CSH attended a number of webinars focusing on providing FSTP and obtaining EU funding (e.g., NCC Workshop organized by the European Commission/ECCC, NCC-SK webinar) and initiated consultations with relevant national stakeholders (for example Technology Centre Prague which acts as the National Contact Point for Horizon Europe) to strengthen knowledge and exchange experiences.

NCISA, in partnership with ENISA, the national accreditation body and other Czech and foreign organizations, conducts awareness-raising events to inform its stakeholders about EU cybersecurity certification. The aim of these events is not only to raise awareness of the upcoming certification programs, but also to establish partnerships within the industry. During a workshop held in November 2022, NCISA informed potential conformity assessment bodies about the possibility of funding their operations through the NCC-CZ, and many organizations expressed interest in this opportunity.

As was already mentioned, both NCISA and CSH are working on setting up mechanisms regarding the FSTP funding management (for example preparing materials, guidelines and internal processes). A project group has been set up in order to ensure capacity and ability to implement this project, bringing together national experts from different departments within NCISA and CSH to provide legal, financial and administrative support.

#§MAT-URI-MU§# #@CON-MET-CM@# #@PRJ-MGT-PM@# #@FIN-MGT-FM@# #@RSK-MGT-RM@#

2.2 Implementation plan and efficient use of resources

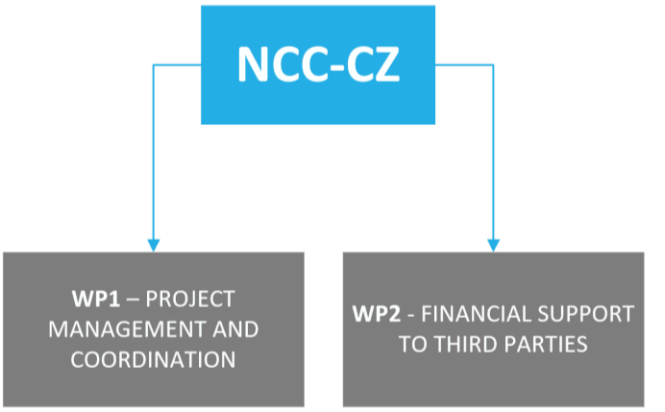
Implementation plan

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.

The work packages (WPs) proposed in this project correspond to the planned project objectives. The main goal is to provide FSTP through the NCC-CZ, therefore WP2 is focusing solely on FSTP. The WP1 focuses on the overall management and coordination of this project that is necessary to perform the tasks and carry out the activities.



WP1 – Project Management and Coordination

The goal of this WP is to manage the project and coordinate the activities taking into account personnel, budget and time during the three-year duration of the project and monitor the progress (disbursement of funds, meeting objectives). The following tasks are envisioned:

- T1.1 Project management: Overseeing the implementation of the project and its activities (meeting objectives, deliverables) and the project budget (reimbursement of funds, expenditures)
- T1.2 Project team coordination: Ensure the project team coordination (division of work and regular meetings to assess the progress of the project and address potential needs), coordination of consortium partners (GA meetings)
- T1.3 EC reporting: Preparing and submitting reports on the progress of the project to the grant authority

WP2 – Financial Support to Third Parties

The objective of WP2 is to set up a financial support program for third parties (FSTP) during the project period, with the aim of supporting the uptake and dissemination of state-of-the-art cybersecurity solutions by SMEs and other entities. The following tasks are planned:

- T2.1 Setting up and adjusting the NCC-CZ FSTP mechanism – Making adjustments to the NCC-CZ FSTP mechanism if necessary.
- T2.2 Preparation of the Strategic Agenda – Identification of the topics to be supported (consulting with relevant entities and taking into account the state of the art and the specific needs of the Czech Republic).
- T2.3 Identification of the pool of expert evaluators – Identify the requirements for evaluators of the project proposals.
- T2.4 Preparation of the open calls and calls activation – Preparation of the Call documentation and activation of the open calls.
- T2.5 Dissemination of information regarding the FSTP calls and information support – Informing the relevant stakeholders about the funding opportunities and the upcoming calls, providing information support for the applicants.
- T2.6 Evaluation of proposals and selection of successful proposals – Evaluation of the project proposals in cooperation with the NCC-CZ Council and expert evaluators, selection of successful projects.

- T2.7 Grant agreement preparation – Prepare the grant agreements with successful applicants for support.
- T2.8 Monitoring of the supported projects, final evaluation and presentation of the project outcomes – Monitor and oversee the supported projects (objectives, progress, grant agreements conditions). Evaluate the project after its end and help disseminate the project outcomes.

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.

The goal is to manage this project effectively and in high quality by overseeing the project's quality control and maintaining communication with both the European Commission and relevant actors. Appropriate mechanisms will be set in order to identify and communicate potentials risks regarding the project, facilitate effective and efficient implementation and reporting in line with the contractual framework and best practices regarding project management. The procedures will be described in the Project Management Handbook (see WP1).

Quality assurance – The project will be managed according to the work plan and all the requirements regarding reporting and information will be fulfilled. Work Package Leaders (WPLs) will be responsible for tasks within work packages (WPs). The General Assembly will coordinate the quality assurance management. General Assembly/project team will meet every six months to perform internal assessments of the project and assure the conformity and quality of all project deliverables with the requirements.

Risk contingency management – The risk management process deals with the identified project risks, ensuring that the consortium fulfils the project goals on time and within the set budget. Project risks will be constantly assessed and evaluated within the duration of the project. The following four steps will be taken:

1. Risk identification
2. Risk evaluation: the probability of events will be determined, and consequences associated with their occurrence will be examined
3. Risk response: mitigation measures will be developed and implemented to reduce or control the risk
4. Risk control and report: lessons learnt will be documented.

All risk management issues will be documented in the Periodic Reports.

Resources management – Project coordinator will take care of the distribution of the financial support amongst the partners in accordance with the Grant Agreement and the consortium agreement. He will also resolve any incorrect, inappropriate, or unauthorised changes during the project duration. Resources Management activities will be focused on:

- operational costs and their reporting,
- the quality regarding the success criteria, the expected specifications and the compliance with best practices,
- the execution time regarding milestones and actual efforts.

Key figures showing the planned versus actual results, efforts, and costs per WP and partner will be internally reported every six months. Internal reporting will be used as a basis for the preparation of the periodic reports towards EC.

Documentation – In order to ensure effective project management, organizational documentation will be created, namely the Coordination Matrix and Workflow Plan. The Coordination Matrix and Workflow plan clearly define the mechanisms for passing on and sharing information, cooperation on individual tasks within the project, the organization of reporting and mechanisms for evaluating activities and outputs, and the processes for their approval. This documentation will be part of the Project Management Handbook and will be periodically revised.

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.*

The financial flows of the project are set using the experience with similar projects (ie. National Cybersecurity Competence Centre, Cybersecurity Innovation Hub, etc.). Based on a consortium agreement, the project coordinator will distribute the funds according to the approved budget. Spending of the grant money in compliance with the project plan and approved budget will be under supervision of WPLs and the project coordinator.

Total estimated expenditures are approximately **856 321 EUR**. The project budget is conceived as adequate and necessary to achieve the planned activities and results of the project. The project includes personnel costs, purchase costs, other cost categories and indirect costs.

The **personnel costs** of the project represent the necessary costs to achieve the planned results of the project, including its management. The composition and structure of the project team reflects long-term experience in managing and implementing strategic projects in the field of ICT and, at the same time, the knowledge, and competencies of key staff, where their excellent representation in the implementation team confirms the strategic importance attached to the project. Personnel costs are calculated, including contributions to social and health insurance premiums and other compulsory expenses and remuneration, and are determined in accordance with the long-term average wage for similar positions and situations in the field of ICT.

The **purchase costs** include travel and subsistence costs (mainly for the domestic travel), equipment costs (for the acquisition of small tangible and intangible assets – computer technology, software, office equipment designed to coordinate and manage the project) and other goods, works and services (for example marketing materials regarding the activities).

Other costs categories include the purchase of services related to networking, dissemination, and marketing activities, such as renting spaces and equipment for events (workshop and final event), streaming services, translation and printing services, communication campaigns (cooperation with media and press offices, direct mailing), the cost of external online tools and systems (video conferencing platforms, etc.). A part of the budget will also be used for the NCC-CZ Council and expert evaluators. Also, the costs for FSTP, as allowed in the call document, constitute a significant part of the budget. The maximum amount per third party is EUR 100 000, in total EUR 500 000 for the budget category FSTP, and the recipients of the FSTP will co-finance the activity by minimum 50 % of the total costs of the activity.

Indirect costs are set at a flat rate of 7 % of the eligible direct costs.

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.*

The tasks of the project will be carried out by a consortium consisting of NCISA and CSH, who together carry out the tasks of the National Coordination Centre in the Czech Republic (NCC-CZ). NCISA will act as the project coordinator (and main beneficiary) and CSH as the affiliated entity.

NCISA is the central administrative body in the Czech Republic for cybersecurity, including the protection of classified information in information and communication systems and cryptographic protection. Within NCISA, the main department responsible for the NCC-CZ is the R&D Unit, however, other departments and subdepartments will provide support, such as the Regulation Department as well as Economy, Project management and Legal departments. The regulatory department of NCISA will offer technical

and professional support for the project. The department's staff has extensive experience in the accreditation and certification field. Also, there are the Czech Republic's representatives in the CCRA development board CCDB, who have completed training at the German Federal Office for Information Security (BSI), and others who are working on the national regulation for cloud services based on the German C5 scheme. This provides them with a technical expertise in the subject.

NCISA is supported by a partner institution CSH in fulfilling the tasks of the NCCs resulting from the 2021/887 Regulation. The cooperation between NCISA and CSH was commenced by signing of the memorandum of cooperation in December 2021. CSH was established by leading Czech universities as an independent non-profit legal entity to support coordination and cooperation in research, application, and innovation projects in the field of cybersecurity. CSHs team has experience in participating in and coordinating large-scale national and international projects (e.g., Czech National Cybersecurity Competence Centre, or CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence, or the Concordia and CyberSec4Europe EU pilot projects), as well as with providing financial support to third parties within the National Cybersecurity Competence Centre (NC3). CSH is also the coordinator of the European Digital Cybersecurity Innovation Hub consortium and has an extensive network of collaborations that includes research organisations, industry, clusters and chambers of commerce, public administrations and international organisations. This experience and the infrastructural, professional and administrative capacities of the CSH will be used in the implementation of relevant project activities.

The project team brings together experts from CSH and NCISA and various departments (R&D, regulation, economic, legal and project management) to ensure the execution of the planned project activities and tasks.

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
[redacted] Project coordinator	NCISA	Responsible for smooth cooperation among consortia members.
[redacted] Project Manager	NCISA	Complex and operational management of the project, i.e. in particular planning of activities, task management, controlling the progress of work within the given schedule and in relation to defined milestones.
[redacted] Project administrator	NCISA	Delivers administration and management support, manages project documentation.
[redacted] Project administrator	NCISA	Ensures complementarity with NCC-CZ activities.
[redacted] Project management and EU funding advisor	NCISA	Supervising and advising in the project management process, providing advice in EU funding.

[redacted] Legal manager	NCISA	Ensures project compliance with national and EU law, coordinates the preparation of contracts, agreements and other legal documents.
[redacted] Legal adviser for public procurement and grant programs	NCISA	Ensures project compliance with national and EU law, coordinates the preparation of contracts, agreements and other legal documents, provides legal advice in the area of public procurement and grant programs.
[redacted] Expert guarantor	NCISA	Provides expertise in cybersecurity certification, cooperates in preparing open calls for third parties, ensures communication with national cybersecurity certification stakeholders.
[redacted] Financial Manager	NCISA	Approving of financial operations, monitoring budget expenditures to ensure alignment with the financial plan of the project.
[redacted] Financial Administrator	NCISA	Ensuring the approval of financial flows as Budget Administrator, managing project financing reports in compliance with national legislation, adhering to methodologies of the Ministry of Finance within the State Budget, ensuring project records in required national information systems.
[redacted] Expert legal consultant	NCISA	Expert legal consultant for EU cybersecurity certification.
[redacted] Expert legal consultant	NCISA	Expert legal consultant for EU cybersecurity certification.
[redacted] Project administrator	CSH	Delivers administration and management support, manages project documentation
[redacted] Financial support	CSH	Provides financial and administrative support to manage funds and other administrative processes, establishes budget and financial plans, ensures economic and financial aspects of public procurement, manages financial risks, sets mechanisms for providing financial support to third parties.
[redacted] Legal support	CSH	Ensures project compliance with national and EU law, coordinates the preparation of contracts, agreements and other legal documents.
[redacted] Project management and EU funding advisor	CSH	Supervising and advising in the project management process, providing advice in EU funding.
[redacted] Project adviser and coordinator of NCC/EDIH activities	CSH	Ensuring the complementarity of activities between NCC-CZ and EDIH, strategic leading of the project, coordinator of activities between NCISA and CSH.

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.

The project tasks will be carried out by CSH and NCISA staff. The goal is to concentrate as many resources as possible in-house through regular employment process/hiring of staff.

Consortium management and decision-making (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.*

NCISA and CSH will incorporate the necessary administrative apparatus and robust management for the project team to function effectively. The project coordinator (NCISA) will be responsible for the coordination and management. The representatives of both consortium partners form the General Assembly, which decides on key organizational issues.

NCISA and CSH closely cooperates within the established expert project team. Cooperation mechanisms including responsibilities will be described in the **Project Management Handbook**. Regular meetings are expected.

Furthermore, project management and decision-making risk will be guided by the terms stipulated in the **Consortium Agreement (CA), Grant Agreement (GA)**, as well as in this project proposal. The aim of the CA is to establish a legal framework for the project to provide clear guidelines for issues within the consortium. The internal decisions will be taken according to the internal documentation of the consortium, namely by the Project Management Handbook (including the already mentioned Coordination Matrix and Workflow Plan). The consortium management is described under the point Project management, quality assurance and monitoring and evaluation strategy in section 2.2. of this document. Decision-making risks are summarized and eliminated under the point of Critical risks and risk management strategy in section 2.2.

#§CON-SOR-CS§# #§QUA-LIT-QL§# #@IMP-ACT-IA@# #@COM-DIS-VIS-CDV@#

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.

The objective of this project is to enhance cybersecurity and resilience of ICT products, processes and services. To accomplish this, the project sets out to construct a comprehensive ecosystem that guarantees professional-grade cybersecurity certification services. Additionally, it aims to assist certification clients, specifically SMEs in fulfilling the specifications outlined by the certification schemes. The funding is expected to:

- Support the capabilities of conformity assessment bodies, and accreditation bodies,
- Improve cybersecurity and interoperability testing abilities,
- Support SMEs in auditing their infrastructure with the aim of improving their cybersecurity protection,
- Facilitate standardization efforts.

KPIs to measure outcomes and deliverables (highly dependent on the interest of third parties):

- At least 1 Certification body (CABs) financially supported to prepare for CRA requirements
- 2 SMEs supported in preparing for CRA certification
- At least 1 training platform focused on CRA capacity building
- Development or implementation of at least 1 supportive service or tool facilitating self-assessment in alignment with the CRA framework (e.g., specialized consultancy service, template documentation, or a technical self-assessment tool).

- At least 4 Guidance or methodical documents created or updated by third party (public awereness materials) in alignment with CRA implementation
- 1 Collaborative initiative launched
- Capacity and knowledge building activities e.g., exchange of best practices among 2 beneficiaries, staff trainings (10 persons),
- 5 Expected supported projects via the FSTP
- 6 Expected e-mail updates
- 2 Expected online/onsite events (approximately 50 participants)
- 6 Expected updates on websites and social media channels (including www.EUcertifikace.nukib.cz etc.)

The communication activities will be planned and prepared based on the Communication and Dissemination Strategy (described in more detail below) which will define the communication channels and target audience etc. The communication activities regarding this project will be also aligned with communication activities of the NCC in the project NCC-CZ (planned newsletters, website updates, direct communication with media etc.).

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.*

A set of different communication channels and tools will be used to disseminate and communicate NCC-CZ activities and the results of the project. The NCC-CZ will together in close cooperation with NCCA target multiple audiences, for example the public, cybersecurity certification stakeholders on the national level, NCC Network, European Community, ECCC and when relevant media.

The NCC-CZ activities will be communicated in close cooperation with the regulatory department of NCISA, which has devised a strategy for securing EU cybersecurity certification, with a primary objective of supporting the establishment of conformity assessment bodies (CABs). To keep the cybersecurity stakeholders informed, the regulatory department communicates updates and developments in the field through emails, webinars, workshops, and/or conferences. During these events, the regulatory department will also provide information about upcoming calls for EU support for cybersecurity certification.

Main communication channels:

- **Web presentation**: Separate website of NCC-CZ will offer information about the activities, news and results of the NCC-CZ regarding this project. Websites of all the partners will be used to publish and widen the information about the NCC-CZ activities and services.
- The EU Certification website will serve as a communication platform where updates on calls for proposals issued by the NCC-CZ to support capacity building of EU cybersecurity certifications will be regularly published.
- **Social media channels:** relevant social media platforms will be used for dissemination of information regarding the NCC-CZ activities and outcomes within this project.
- **PR articles published in cooperating media:** Especially printed and/or electronic media focusing on cybersecurity and the target audience.
- **Direct communication with media**: Interviews provided by the representatives of NCC-CZ, press releases (regarding the start of the project, new activities and major outputs)
- **Direct communication with partners and stakeholders**: Sharing of information within the national cybersecurity certification stakeholders via direct e-mails or newsletters.

Communication tools:

- **Direct mailing campaigns**: through newsletters and other direct e-mails addressed to potential participants and relevant partners
- **Printed and online PR campaign**: Traditional tools such as press releases, interviews with media, articles in the expert/targeted media will be applied and accompanied by modern PR tools social media.
- **Direct mailing campaigns:** Through newsletters and other direct e-mails addressed to potential participants and relevant national stakeholders.

All the communication activities will be implemented in a standardized manner, relying not only on the NCC-CZ partners experiences and communication standards but also on the internal documentation:

- **Communication and Dissemination Plan** – A sophisticated plan will be elaborated at the beginning of the project taking into account the rules regarding visibility (using a visible EU logo) and quality of information and building upon experience of the project partners with communication and dissemination strategies. This plan will include the comprehensive dissemination and communication strategy, will focus on needs and expectations of target groups, and will plan their engagement and will set the dissemination and communication overall approach, project partners responsibilities, the framework of cooperation and describe in more particular the dissemination and communication channels/tool according to their importance. It will also cover the exploitation.

- **Marketing materials –** A basic set of marketing materials illustrating the services provided by NCISA and CSH to attract the target groups will be created.

#§COM-DIS-VIS-CDV§#

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

Certification, which consists of the evaluation of products, services and processes by an independent and accredited body against a defined set of criteria and the issuing of a certificate indicating conformance is crucial for increasing security in products, processes and services and, therefore, trust in these products, processes and services. With cybersecurity requirements being seen as essential to safeguard the benefits of the evolving digitalisation of society, and given the rapid proliferation of connected devices, certification serves to inform and reassure purchasers and users about the security properties of the ICT products and services that they buy or use. Risks related to the supply chain security may be significantly mitigated. If there is a bigger trust in the products and services offered, they can be better marketed. Certification also helps with protecting data (whether stored, transmitted or otherwise processed) against accidental or unauthorised storage, processing, access, disclosure, destruction, accidental loss or alteration.

Ensuring national certification capacities can lead to increased trust and security, especially from the local point of view. By developing and enhancing the testing and certification capabilities and capacities in the Czech Republic, companies will not be required to engage in certification process outside of the country which would allow them to save on costs. This could be of a great benefit especially to small and medium-sized enterprises which have limited resources. The security ensured by the Czech Republic would be increased which would contribute to a better security of EU as such. However, we understand, that developing and enhancing the testing and certification capabilities and capacities in the Czech Republic contributes to the effort for building a common European system of cybersecurity certifications, therefore we expect entities from other eligible European countries to the degree possible and sensible, to benefit from the NCC-CZ calls. Also, our actions will be coordinated with other NCCs to exchange best practices, avoid overlapping capacities, contribute to the common goal and have a greater outreach at EU level.

3.3 Environmental sustainability and contribution to European Green Deal goals

Environmental sustainability and contribution to European Green Deal goals

Describe the extent to which the project will contribute to environmental sustainability and in particular to European Green Deal goals

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

Not applicable as stated in the Call document DIGITAL-ECCC-2022-CYBER-03.

#§IMP-ACT-IA§#

#@WRK-PLA-WP@#

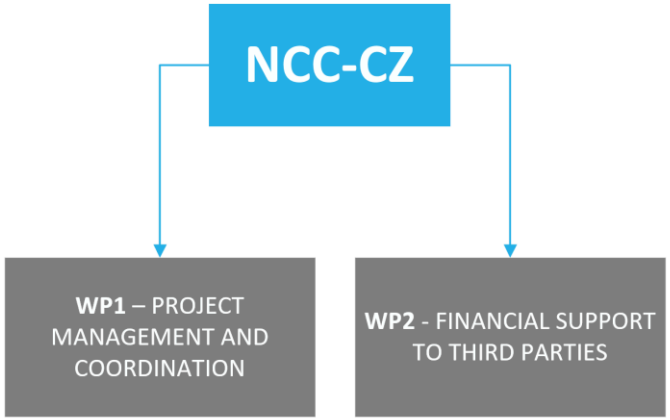
4. WORK PLAN, WORK PACKAGES, ACTIVITIES, RESOURCES AND TIMING

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)).

In the figure below, the overall structure of the planned WPs is given. The work plan of this project will consist of fulfilling the project objectives. Two WPs are set, the first one focusing on project management and coordination of the whole project, and the second WP covering the financial support to third parties (FSTP). Details regarding the individual WPs including the planned objectives, tasks, milestones and deliverables as well as budgetary information are available in section 4.2 below. WP2 covering FSTP includes both the personnel costs for the tasks as well as the budget for the FSTP.



4.2 Work packages, activities, resources and timing

Work Package 1

Estimated budget — Resources *(n/a for prefixed Lump Sum Grants)*												
Participant	Costs											
	A. Personnel		B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties		D.2 Internally invoiced goods and services	D.3 PAC procurement costs *(for PAC Grants for Procurement)*	E. Indirect costs	Total costs
NCISA	17 person months	56100 EUR	0 EUR	2000 EUR	4000 EUR	0 EUR	0 grants	0 EUR	0 EUR	0 EUR	4347 EUR	66447 EUR
CSH	6 person months	30000 EUR	0 EUR	2000 EUR	4000 EUR	0 EUR	0 prizes	0 EUR	0 EUR	0 EUR	2520 EUR	38520 EUR
Total	23 person months	86100 EUR	0 EUR	4000 EUR	8000 EUR	0 EUR	0 grants 0 prizes	0 EUR	0 EUR	0 EUR	6867 EUR	104967 EUR

Work Package 2

Estimated budget — Resources *(n/a for prefixed Lump Sum Grants)*												
Participant	Costs											
	A. Personnel		B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties		D.2 Internally invoiced goods and services	D.3 PAC procurement costs *(for PAC Grants for Procurement)*	E. Indirect costs	Total costs
NCISA	34 person months	112200 EUR	0 EUR	1000 EUR	0 EUR	13000 EUR	5 grants	500000 EUR	0 EUR	0 EUR	43834 EUR	670034 EUR
CSH	15 person months	75000 EUR	0 EUR	1000 EUR	0 EUR	0 EUR	0 grants	0 EUR	0 EUR	0 EUR	5320 EUR	81320 EUR
Total	49 person months	187200 EUR	0 EUR	2000 EUR	0 EUR	13000 EUR	5 grants 0 prizes	500000 EUR	0 EUR	0 EUR	49154 EUR	751 354 EUR

Subcontracting (n/a for prefixed Lump Sum Grants)

Subcontracting

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

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

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

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

Work Package No	Subcontract No (continuous numbering linked to WP)	Subcontract Name (subcontracted action tasks)	Description (including task number and BEN/AE to which it is linked)	Estimated Costs (EUR)	Justification (Why is subcontracting necessary?)	Best-Value-for-Money (How do you intend to ensure it?)
N/A	S1.1	-	-	-	-	-
N/A	S1.2	-	-	-	-	-

Other issues: *If subcontracting for the entire project goes beyond 30% of the total eligible costs, give specific reasons.*	N/A

Purchases and equipment

Purchase costs (travel and subsistence, equipment and other goods works and services)

Details for major cost items (needed if costs declared under 'purchase costs' are higher than 15% of the claimed personnel costs).

Start with the most expensive cost items, down to the 15% threshold.

Participant 1:	NCISA			
Cost item name	Category	WP(s)	Explanations	Costs (EUR)

N/A	-	-	-	-
			Total	-
Participant 2:	CSH			
Cost item name	Category	WP(s)	Explanations	Costs (EUR)
N/A	-	-	-	-
			Total	-
			Total	-
			Total purchase costs > 15% (all participants)	-
			Remaining purchase costs < 15% (all participants)	-
			Total purchase costs (all participants)	-

Equipment with full-cost option

For calls where full-capitalised costs are exceptionally eligible for listed equipment (see Call document), indicate below the equipment items for which you request the full-cost option, and justify your request. Ensure consistency with the budget details provided in the previous table.

Equipment Name	Description (including WP, task number and BEN/AE to which it is linked)	Estimated Costs (EUR)	Justification (why is reimbursement at full-cost needed?)	Best-Value-for-Money (how do you intend to ensure it?)
N/A	-	-	-	-
N/A	-	-	-	-

Other cost categories

Other cost categories (financial support to third parties, internally invoiced goods and services, etc) *Complete the table below for each participant that would like to declare costs under other costs categories (e.g. financial support and internally invoiced goods and services), irrespective of the percentage of personnel costs.*		
Participant 1:	NCISA	
Cost category	Explanations	Costs (EUR)
Financial support to third parties	The goal of this project proposal is to provide FSTP to relevant stakeholders with the aim to support building testing and certification capabilities in the Czech Republic.	500000
Internally invoiced goods and services	-	-
Participant 2:	CSH	
Cost category	Explanations	Costs (EUR)
Financial support to third parties	-	-
Internally invoiced goods and services	-	-

Timetable

Timetable (projects of more than 2 years)

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

Note: *Use actual calendar years and quarters. In the timeline you should indicate the timing of each activity per WP. You may add additional columns if your project is longer than 6 years.*

ACTIVITY	YEAR 1				YEAR 2				YEAR 3				YEAR 4
	Q 1	Q 2	Q 3	Q 4	Q 1	Q 2	Q 3	Q 4	Q 1	Q 2	Q 3	Q 4	Q 1
Task 1.1 - Project management													
Task 1.2 - Project team coordination													
Task 1.3 - EC Reporting													
Task 2.1 - Setting up and adjusting the NCC-CZ FSTP mechanism													
Task 2.2 - Preparation of the Strategic Agenda													
Task 2.3 - Identification of the pool of expert evaluators													
Task 2.4 - Preparation of the open calls and its activation													
Task 2.5 - Dissemination of information regarding the FSTP calls and information support													

Task 2.6 - Evaluation of proposals and selection of successful proposals													
Task 2.7 - Grant agreement preparation													
Task 2.8 - Monitoring of the supported projects, final evaluation and presentation of the project outcomes													

#§WRK-PLA-WP§#

#@ETH-ICS-EI@#

5. OTHER

5.1 Ethics

Ethics

If the Call document contains a section on ethics, the ethics issues and measures you intend to take to solve/avoid them must be described in Part A.

Ethical dimension of the objectives, methodology and likely impact

The project does not involve any ethics issues that would invoke the need for ethics self-assessment. Therefore, it has not entered any ethics issues in the ethical issue table in the administrative proposal forms. However, we note that all work carried out under the project will respect fundamental ethics principles, including those reflected in the Charter of Fundamental Rights of the European Union, the relevant ethics rules of European Commission projects, and national and European laws. Ethics will be monitored during the project in WP 1 and 2.

Compliance with ethical principles and relevant legislation

The project ethics requires all partners contributing to the project to comply with the letter and spirit of any laws, legislation and guidelines that apply and to implement all tasks to the highest ethical behaviour and standards. Each partner shall implement their project tasks with total respect and highest regard for their organisational colleagues, fellow partners and project participants. The project will be implemented in a professional manner without any form of prejudices whatsoever, irrespective of gender, race, ethnic background, religion, nationality, geography, colour or creed.

The project coordinator, National Cyber And Information Security Agency, will be monitoring ethics that the project will leverage.

Good ethical governance and review of research and innovation is a core value and priority at NCISA. It is the responsibility of the NCISA and project partner to scrutinise all projects that involves humans to ensure it is compliant with statutory requirements and is conducted to the highest ethical principles, which emphasise the rights and welfare of subjects, treating all with dignity and ensuring that those who participate in research, whether subjects, researchers, other stakeholders are not put at risk project will leverage.

Additionally, all activities will be carried out ensuring ethical principles in accordance with Directive 95/46/EC of the European Parliament and also in accordance with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). All national data protection and privacy laws will also be followed.

Confirmations

I confirm that compliance with ethical principles and applicable international, EU and national law in the implementation of research activities not originally envisaged (or not described in detail) in the DoA will be ensured.

I confirm that any ethical concerns raised by those activities will be handled following rigorously the recommendations provided in the European Commission Ethics Self-Assessment Guidelines.

#§ETH-ICS-EI§# #@SEC-URI-SU@#

5.2 Security

Security

The security issues and the measures you intend to take to solve/avoid them must be described in Part A.

***Note:** Beneficiaries must ensure that their projects are not subject to national/third country security requirements that could affect the implementation or put into question the award of the grant (e.g. technology restrictions, national security classification, etc).*

See Application Form Part A.

#§SEC-URI-SU§# #@DEC-LAR-DL@#

6. DECLARATIONS

Double funding	
Information concerning other EU grants ⚠ *Please note that there is a strict prohibition of double funding from the EU budget (except under EU Synergies actions).*	**YES/NO**
We confirm that to our best knowledge none of the projects under the action plan as a whole or in parts have benefitted from any other EU grant *(including EU funding managed by authorities in EU Member States or other funding bodies, e.g. EU Regional Funds, EU Agricultural Funds, etc)*. If NO, explain and provide details.	YES
We confirm that to our best knowledge none of the projects under the action plan as a whole or in parts are (nor will be) submitted for any other EU grant *(including EU funding managed by authorities in EU Member States or other funding bodies, e.g. EU Regional Funds, EU Agricultural Funds, etc)*. If NO, explain and provide details.	YES

Financial support to third parties (if applicable) *If in your project the maximum amount per third party will be more than the threshold amount set in the Call document, justify and explain why the higher amount is necessary in order to fulfil your project's objectives.*
Not applicable, the maximum amount per third party is set within the threshold amount set in the Call document.

#§DEC-LAR-DL§#

ANNEXES

LIST OF ANNEXES

Standard
Detailed budget table/Calculator (annex 1 to Part B) — *mandatory for certain Lump Sum Grants (see Portal Reference Documents)*
CVs (annex 2 to Part B) — *not applicable*
Annual activity reports (annex 3 to Part B) — *not applicable*
List of previous projects (annex 4 to Part B) — *mandatory, if required in the Call document*

Special
Other annexes (annex 5 to Part B) — *mandatory, if required in the Call document*

LIST OF PREVIOUS PROJECTS

List of previous projects *Please provide a list of your previous projects for the last 4 years.*					
Participant	Project Reference No and Title, Funding programme	Period (start and end date)	Role (COO, BEN, AE, OTHER)	Amount (EUR)	Website (if any)
N/A	Not applicable as stated in the Call document DIGITAL-ECCC-2022-CYBER-03.	-	-	-	-

HISTORY OF CHANGES		
VERSION	PUBLICATION DATE	CHANGE
1.0	01.11.2021	Initial version (new MFF).

DATA SHEET

1. General data

Project summary:

Project summary
The objective of this project is to increase and facilitate security and interoperability of testing capabilities and certification of connected ICT systems by cascade funding provided by the NCC-CZ. This aims to improve the capabilities and cooperation of cybersecurity certification stakeholders in line with the objectives of Regulation (EU) 2019/881 (“CSA”).

Keywords:

- Cybersecurity
- NCC, FSTP, Cascade Funding, Cybersecurity Certification

Project number: 101127940

Project name: Building Testing and Certification Capabilities in the Czech Republic

Project acronym: TEST-CERT-CZ

Call: DIGITAL-ECCC-2022-CYBER-03

Topic: DIGITAL-ECCC-2022-CYBER-03-TEST-CERT-CAPABILTIES

Type of action: DIGITAL JU Grants for Financial Support

Granting authority: European Cybersecurity Industrial, Technology and Research Competence Centre

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

Project starting date: fixed date: 1 December 2023

Project end date: 28 February 2027

Project duration: 39 months

Consortium agreement: Yes

2. Participants

List of participants:

N°	Role	Short name	Legal name	Ctry	PIC	Total eligible costs (BEN and AE)	Max grant amount	Entry date	Exit date
1	COO	NCISA	NARODNI URAD PRO KYBERNETICKOU A INFORMACNI BEZPECNOST - NUKIB	CZ	907198418	736 481.00	721 921.00		
1.1	AE	CSH	CYBERSECURITY HUB, ZU	CZ	889292509	119 840.00	119 840.00		
Total						856 321.00	841 761.00		

Coordinator:

- NARODNI URAD PRO KYBERNETICKOU A INFORMACNI BEZPECNOST - NUKIB (NCISA): from 1 December 2023 to present

3. Grant

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

Total eligible costs (BEN and AE)	Funding rate (%)	Maximum grant amount (Annex 2)	Maximum grant amount (award decision)
856 321.00	100	841 761.00	841 761.00

Grant form: Budget-based

Grant mode: Action grant

Budget categories/activity types:

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

- B. Subcontracting costs

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

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

- E. Indirect costs

Cost eligibility options:

- Standard supplementary payments

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

- Country restrictions for subcontracting costs

- Limitation for subcontracting

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

- Equipment: depreciation and full costs for listed equipment

- Costs for providing financial support to third parties (actual cost; max amount for each recipient: EUR 100 000.00)

- 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	21	Additional prefinancing report	60 days after end of reporting period	Additional prefinancing	60 days from receiving additional prefinancing report/ financial guarantee (if required) – whichever is the latest
2	22	39	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)	589 232.70	n/a	1 - NCISA	n/a
			1.1 - CSH	n/a
Prefinancing 2 (additional)	168 352.20	n/a	1 - NCISA	n/a
			1.1 - CSH	n/a

Reporting and payment modalities (art 21, 22):

Mutual Insurance Mechanism (MIM): No

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

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

No-profit rule: Yes

Late payment interest: ECB + 3.5%

Bank account for payments:

[redacted]

Conversion into euros: Double conversion

Reporting language: Language of the Agreement

4.3 Certificates (art 24):

Certificates on the financial statements (CFS):

Conditions:

Schedule: only at final payment, if threshold is reached

Standard threshold (beneficiary-level):

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

4.4 Recoveries (art 22)

First-line liability for recoveries:

Beneficiary termination: Beneficiary concerned

Final payment: Coordinator

After final payment: Beneficiary concerned

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

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

Joint and several liability of affiliated entities — n/a

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

Applicable law (art 43):

Standard applicable law regime: EU law + law of Belgium

Dispute settlement forum (art 43):

Standard dispute settlement forum:

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

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

6. Other

Specific rules (Annex 5): Yes

Standard time-limits after project end:

Confidentiality (for X years after final payment): 5

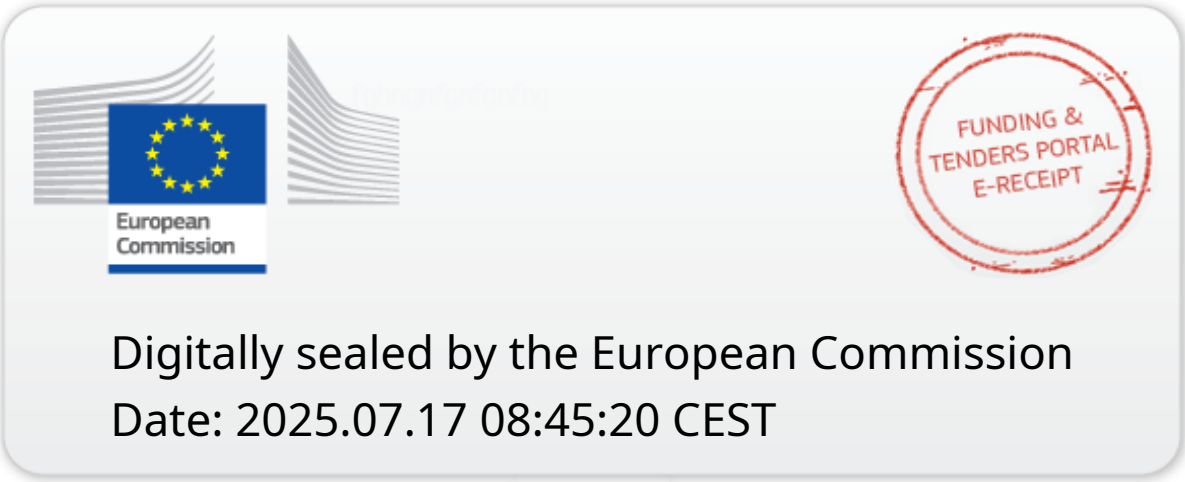
Record-keeping (for X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)

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

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

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

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



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)