SECURE
Cyber Resilience for SMEs

ANNEX 1 - SECURE SECOND OPEN CALL FOR PROPOSALS GUIDELINES



Funded by the European Union

EU Funding Statement: Funded by the European Union under GA No 101190325. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Industrial, Technology and Research Competence Centre.
Neither the European Union nor the granting authority can be held responsible for them.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

ECCC disclaimer: The Project is supported by the European Cybersecurity Competence Centre and its members

Versioning Disclaimer: this version of the Call Guidelines faithfully reflects the content of project deliverable 2.3 as will be submitted on the EU Tender platform.
Only graphic enhancements have been introduced to improve readability for the applying SMEs.

Table of Contents

ANNEX 1 - SECURE SECOND OPEN CALL FOR PROPOSALS GUIDELINES 1

SECURE-CALL #2- Open Call for Proposals 4

The SECURE Project 4

Publication Notice 5

Definitions & Acronyms 6

1. SECURE Second Open Call: Scope and Details 8

1.1. Objectives 8

1.2. Scope 8

1.3. Financial Support & Payments 9

1.4. Support from National Authorities during application – The Role of the NCCs 10

1.5. Language and Tools 10

2. Eligibility Requirements 11

2.1. Company Eligibility Criteria 11

2.2. CRA-related Requirements 11

PROPOSAL & PROJECT SUBMISSION PROCESS 13

3. STAGE 1 - Registration & Proposal submission process 14

3.1. PHASE 1 – Registration & Company Documentation Upload 14

3.2. PHASE 2 – Proposal & Budget drafting 15

3.3. PHASE 3 – Proposal Evaluation 16

3.4. PHASE 4 – Sub-Grant Agreement (Sub-GA) Signing 19

4. STAGE 2 - Project Implementation and Technical Report Submission Process 20

4.1. PHASE 5 – Initial CRA Maturity Assessment 20

4.2. PHASE 6 – Implementation & Technical Report 21

4.3. PHASE 7 – Implementation Assessment, Payment & Attestation 21

5. Communications and Information 22

6. Mandatory Annexes and Supporting Documents 23

Appendix A – Company Eligibility Criteria 24

A. Individual Entities 24
B. mSMEs definition 24
C. Geographical Eligibility 25
D. Legal and ethical requirements and exclusions 26
E. Double funding exclusion 27
APPENDIX B - Proposal Technical Evaluation *28*
A. Evaluation Committee 28
B. Proposal Evaluation Criteria 28
C. Proposal Scoring 30
APPENDIX C - Implementation Assessment *32*
A. Project Implementation & Technical Report Assessment 32
B. Implementation Evaluation Outcomes 32

SECURE-CALL #2- Open Call for Proposals

Financial Support for CRA Compliance

The SECURE Project

SECURE – Strengthening EU SMEs Cyber Resilience Project (Grant Agreement No. 101190325) is a three-year Project that started in January 2025, funded by the European Union under the Digital Europe Programme (DIGITAL-ECCC-2024-DEPLOY-CYBER-06, topic STRENGTHENCRA).

The purpose of SECURE is to reinforce the cybersecurity resilience of European micro, small and medium-sized enterprises (mSMEs) by helping them comply with the requirements of the Cyber Resilience Act (CRA) through the launch of Open Calls. These will provide direct financial support to co-finance concrete Projects aimed at improving CRA compliance and enhancing cybersecurity practices. In addition to financial support, the Project will deliver a set of complementary actions. It will develop a digital platform that will act as the central access point for Open Calls and as a shared repository of CRA-related tools, resources, and training materials, supporting a consistent and practical approach to cybersecurity resilience across the EU. SECURE will also promote awareness and capacity-building through workshops, training sessions, and events designed to share best practices and foster engagement among the SME community. Furthermore, the Project will contribute to standardisation efforts, drawing on the practical needs and experiences of SMEs to support the development of harmonised standards for the effective implementation of the CRA. Over the course of the Project, the Consortium will launch a series of Open Calls through which cascade funding will be distributed to mSMEs across the European Union. These calls are designed to co-finance concrete Projects aimed at improving CRA compliance, strengthening cybersecurity practices, and promoting a harmonised approach to resilience throughout the EU.

The Project is coordinated by the **Agenzia per la Cybersicurezza Nazionale (ACN)** and includes the following partners:

- **Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK, Poland)**
- **Instituto Nacional de Ciberseguridad de España – INCIBE (Spain),**
- **Centre for Cybersecurity Belgium – CCB (Belgium)**
- **Luxembourg House of Cybersecurity – LHC (Luxembourg),**
- **Associazione Cyber 4.0 (Italy)**
- **Autoritatea pentru Digitalizarea României – ADR (Romania),**
- **Industrie 4.0 Österreich – Plattform für Intelligente Produktion (PIA, Austria).**

The partnership includes **National Cybersecurity Coordination Centres (NCCs)**, research organisations, and technical actors, ensuring a wide geographical coverage and a strong combination of institutional and operational expertise.

Publication Notice

SECURE-CALL#2 - CALL PUBLICATION NOTICE	
Call ID	SECURE-CALL #2 - SECURE Second Open Call For Proposals
Call Description	Financial support for mSMEs to co-finance activities, goods, and services aimed at strengthening cyber resilience and achieve the compliance with the Cyber Resilience Act.
Call Publication	01/10/2026
Call Deadline	29/01/2027
Call Total Budget	EUR 11,500,000[1]
Funding Body	European Union and European Cybersecurity Competence Centre through CONSORTIUM SECURE Project, Coordinated by the Agenzia per la Cybersicurezza Nazionale (ACN)
Eligible Applicants	mSMEs based in one of the Eligible Countries – Reference to Eligibility Chapter
Expected duration of Projects	Maximum: 180 calendar days
Cofinancing Rate	Projects will be co-financed at a rate of 50%, up to a maximum contribution of EUR 30,000. This ceiling applies also to Projects with total eligible costs higher than EUR 60,000
Maximum amount of funding per Project	EUR 30,000
Form of grant	Lump sum
Weblink for further information	https://secure4sme.eu/#cascade
Contact	submission-support@secure4sme.eu

[1] The total budget indicated represents the minimum amount available and may be increased through the reallocation of any unspent funds from the previous call.

Definitions & Acronyms

Name/Acronym	Definition
Applicant or Applicant's Company	A company, organisation or self-employed person applying for a Call published under the SECURE Project. The status of "Applicant" refers to mSMEs submitting a co-financing request for a Project related to CRA compliance, by providing the required information, Project costs, and the Project Proposal.
Beneficiary Company	Applicants whose Projects successfully pass the evaluation phases and sign the Sub-Grant Agreement acquire the status of "Beneficiaries".
CRA	Cyber Resilience Act - Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements
ECCC	European Cybersecurity Competence Centre
EU	European Union
ENISA	European Union Agency for Cybersecurity
Ev.Co.	Evaluation Committee
Executive management structure	A body appointed in accordance with national law, and, where applicable, reporting to the chief executive officer, which is empowered to establish the strategy, objectives and overall direction, and who oversees and monitors management decision-making.
Financial Regulation	Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast), as amended
GBER	General Block Exemption Regulation - Commission Regulation (EU) 651/2014 declaring certain categories of aid compatible with the internal market in application of Articles 107 and 108 of the Treaty
Headquarters/ Global Headquarters	The place where the Applicant's central administration is effectively located, as determined by the actual exercise of its overall executive management and strategic decision-making functions
ICT	Information and Communication Technology
IoT	Internet of Things
IT	Information Technology
KPI	Key Performance Indicator
Legal establishment or place of establishment	The country in which the Applicant is legally established, as evidenced by an entry in the relevant official register or, where registration is not required under applicable law, by equivalent documentation issued by a competent authority.
Main business operations	The Applicant's principal place of business, meaning the country in which it carries out the principal part of its business activities
mSMEs	Micro, Small and Medium Enterprises, as defined in the Annex to Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

NCC	National (Cybersecurity) Coordination Centre
OT	Operational Technology
PAdES	PDF Advanced Electronic Signatures. A set of standards that extend PDF format to support advanced and qualified electronic signatures, ensuring authenticity, integrity, and legal validity of digital documents in compliance
Qualified Electronic Signature (QES)	An advanced electronic signature that is created by a qualified electronic signature creation device and which is based on a qualified certificate for electronic signatures, as defined and regulated by Regulation (EU) No 910/2014 (eIDAS), in particular Article 3(12) thereof. For the purposes of these Guidelines and the relevant application documents, references to "digital signature" or "digitally signed" shall be understood as references to a Qualified Electronic Signature (QES).
SECURE	Strengthening EU SMEs Cyber Resilience - Project that supports European mSMEs to strengthen EU Cyber-Resilience
Sub-GA	Sub-Grant Agreement - Document that defines the contractual terms the Applicant must accept to receive the funding. The prefix "sub" indicates that the Grant Agreement signed by the Applicants is legally dependent on the Grant Agreement signed by the SECURE consortium partners for the allocation of funds.
WP	Work Package

1. SECURE Second Open Call: Scope and Details

1.1. Objectives

SMEs are the backbone of Europe's economy and of its digital single market, making them among the most exposed to cyber risks. However, they often lack the financial and technical capacity to adapt to new regulatory obligations. Therefore, the main objective of this Call is to provide financial support to European mSMEs in achieving compliance with the CRA and in strengthening their overall cybersecurity resilience.

Eligible Projects under this Call must have the clear objective of strengthening the cyber resilience of the Applicant Company's processes, products, technologies, infrastructures, or services, with the ultimate goal of achieving compliance with the CRA.

1.2. Scope

The **Cyber Resilience Act (CRA)**, Regulation (EU) 2024/2847, entered into force on **10th December 2024**, with its main obligations applying from **11 December 2027** and Article 14 reporting obligations applying from 11 September 2026 and establishes common cybersecurity requirements for products with digital elements made available on the EU market within its scope. Its goal is to ensure that digital products are maintained and supported in accordance with the applicable essential cybersecurity requirements, thereby increasing trust and transparency for both businesses and consumers.

The CRA applies to a wide range of products, provided they are connected, either directly or indirectly, to other devices or networks. Exclusions apply to specified products covered by the legislation listed in Article 2(2)-(4), including aviation products certified under Regulation (EU) 2018/1139. Products complying with CRA requirements will carry the **CE mark**, enabling users to identify solutions meeting EU cybersecurity standards.

The CRA imposes clear obligations for **manufacturers (including software developers meeting Article 3(13)), authorised representatives, importers and distributors (including retailers),** covering all phases of the product lifecycle — from design and development to updates, maintenance, and end-of-life. For certain important and critical products with digital elements, the applicable conformity assessment procedure may require third-party involvement, depending on the product classification and on the conformity assessment route applicable under the CRA.

Therefore, as a first step, Companies wishing to apply to this Call, should verify whether they currently fall, or are expected to fall in the future, under the main categories of entities subject to the obligations of the CRA Regulation.

According to these requirements, proposed Projects and related funding requests under this Call, may cover different types of activities carried out by company personnel or by external providers (as subcontracting costs), provided they aim to support the Applicant Company in meeting the requirements of the CRA, including:

- **Regulatory compliance activities**, such as audits, activities supporting applicable conformity assessment procedures and, where relevant, cybersecurity schemes, and policy definition.
- **Product-related technological and security requirements upgrading**, through activities such as vulnerability assessment and penetration testing, source code analysis, and application security.

- **Upgrading of technological and security requirements of production infrastructures**, including cybersecurity, information security, ICT, IT, and OT resilience activities demonstrably linked to the security of identified in-scope products and the relevant CRA obligations.
- **Fulfilling internal governance and risk management requirements**, such as internal procedures, incident detection, management and notification processes, risk and impact assessments, supply chain security and product maintenance and updating plans.
- **Awareness raising and training activities** on products and cyber security.
- **Procurement of material goods and professional services** that are instrumental to achieving the required security standards.

A detailed description of CRA scope and a more comprehensive list of fundable activities, services and goods are provided in the ***ANNEX 2-CRA Scope & Eligible Activities, Services and Goods.***

1.3. Financial Support & Payments

The estimated budget for the SECURE Call 2 - *SECURE-CALL #2 - SECURE Second Open Call For Proposals* - is EUR 11,500,000. The SECURE Consortium reserves the right to increase the total call budget depending on any unallocated funds from the previous call.

Successful Applicants will receive a **grant covering 50% of the total eligible costs of their Project**, up to a **maximum SECURE contribution of EUR 30,000**. **If the total Project cost exceeds EUR 60,000, the SECURE contribution will remain capped at EUR 30,000.**

The grant is awarded to enable mSME to implement the action described in ***ANNEX 1.1-Proposal Template***, (later, ***ANNEX 5-Sub-Grant Agreement***).

Given the fact the Grant is awarded with EU funds, it does not fall under the *de minimis* aid regime nor under the General Block Exemption Regulation (GBER).

Payments will normally be made in two instalments:

- **Pre-financing**: an optional pre-financing payment of 40% of the grant may be made upon signing the Sub-Grant Agreement, or within few days later, if requested by the company at Proposal submission.
- **Balance**: Companies that request pre-financing will receive the remaining balance after Project completion and approval of the final Technical Report. Companies not requesting pre-financing will receive the full payment only after Project completion and approval of the final Technical Report.

The full payment of the grant is conditional on the successful implementation of all activities and the attainment of the Milestones and KPIs (Key Performance Indicators) specified in the application and confirmed in the Sub-Grant Agreement signed with Cyber 4.0. Should the final evaluation reveal gaps, partial fulfilment, or unsatisfactory results, the grant may be reduced. Poor, incomplete, or delayed implementation can lead to a flat-rate reduction. Based on the overall Project assessment, the Evaluation Committee may apply a proportionate decrease to the total grant, in line with the standard scale described in the **Appendix C.**

If, during the Project implementation evaluation, it is determined that the Milestones and KPIs have not been achieved at all— regardless of the costs already incurred by the beneficiary — the final payment will not be made. If the pre-financing has already been issued, the beneficiary will be required to reimburse it in case the agreed objectives and Milestones are not met.

Eligible costs and are described in the ***ANNEX 1.2-Proposal Budget Guidelines***.

Under the SECURE Call, **lump sum** grants are applied. This means that the grant amount is fixed and will be paid if the Project is implemented as agreed. Applicants are nevertheless required to provide a breakdown of the underlying costs in the Proposal budget form, as the eligibility and reasonableness of such costs are assessed during the evaluation of the Proposal. At the end of the Project, beneficiaries must demonstrate the

activities carried out and provide evidence that the planned Milestones and KPIs have been achieved. No detailed financial reporting is required. However, the European Commission may still perform financial checks and audits. Beneficiaries are therefore required to keep proper documentation on usual financial practices and procedures, as well as records on the financial and technical implementation of the Project (i.e. costs incurred and activities implemented), to provide evidence of compliance if requested.

1.4. Support from National Authorities during application – The Role of the NCCs

The **National Cybersecurity Coordination Centres (NCCs)**, established under Regulation (EU) 2021/887 alongside the **European Cybersecurity Competence Centre (ECCC)**, form a central pillar of the EU cybersecurity strategy. While the ECCC manages initiatives and resources at the European level, NCCs act as local anchors in each Member State, supporting enterprises, academia, and public authorities. Their mandate includes fostering national cybersecurity ecosystems, strengthening collaboration across industry, research, and the public sector, promoting participation in European cybersecurity Projects, and ensuring alignment with EU strategic objectives. For the complete list of EU NCCs, please visit: https://cybersecurity-centre.europa.eu/nccs_en.

In the context of the SECURE Project, the NCCs will play a key role by supporting local enterprises during the submission phase and assisting in the evaluation of their eligibility for funding. To do that, in addition to consortium members, the SECURE Project actively involved the wider network of NCCs, obtaining endorsement from the majority of them.

Within the SECURE Project, NCCs are responsible for conducting the eligibility check of the Applicant Companies. Therefore, companies based in a Member State whose NCC does not support the SECURE Project Call may still submit a Project Proposal, but there is no guarantee that their application will pass the Company Eligibility checks phase, as the NCC cannot perform the required validation. To this end, before submitting a Proposal, Applicants are strongly recommended to verify if the NCC in their respective country are involved in the call, also by directly contacting them before applying. Any update regarding the involvement of the NCCs in the present Project will be provided through the SECURE Platform, official site and communication channels of the SECURE Project.

1.5. Language and Tools

Any documentation submitted or shared in the framework of this Open Call shall be provided in English, except for official documents issued by public administrations or competent authorities of the Member State in which the Applicant Company is established. For the submission of the Technical Proposal, Applicants must exclusively use Annex 1.1 Proposal Template and Annex 1.3 Proposal Budget Template.

The Call is managed through an online platform that handles the entire process, including registration, Proposal submission, evaluation, funded Projects implementation, and impact assessment, ensuring accessibility, transparency, and security.

All documents and templates to be used by Applicants are listed in these Guidelines and must be followed carefully. Failure to comply with the applicable requirements may result in the Proposal being considered inadmissible.

In order to obtain EU funding, Applicants must comply with these Guidelines. Applications must be complete, concise, and submitted within the applicable deadline through the SECURE electronic submission portal.

2. Eligibility Requirements

To be eligible for the present Call, Applicants must fulfil both of the following conditions:

- **Company Eligibility criteria** and
- **CRA-related requirements**.

2.1. Company Eligibility Criteria

To be eligible for the present Call, Applicants must not fall under any of the exclusion criteria and must comply cumulatively with the following requirements:

- **Be individual legal entities**.
- **Qualify as a Micro, Small or Medium-sized Enterprise (mSME)**.
- **Comply with the Geographical eligibility criteria set out in point (c) of Appendix A.**
- **Meet all relevant legal and ethical requirements**.
- **Ensure that the proposed Project is not subject to double funding**.

Failure to meet any of the company eligibility criteria will result in the exclusion of the Applicant from funding. **For further information on Company eligibility requirement and specific cases, please refer to Appendix A** of this document (for any additional reference please check https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/guidance-on-participation-in-eu-calls-with-ownership-and-control-restrictions_en.pdf).

National Cybersecurity Coordination Centres (NCCs) that have committed their support to the SECURE Project will evaluate compliance with company eligibility criteria. Each NCC, in line with its institutional mandate, will support mSMEs in its Member State during the application process and are responsible for verifying compliance with the company eligibility requirements. If the eligibility evaluation is not carried out by the NCC of the relevant Member State, the submitted Proposal may be declared ineligible for funding.

2.2. CRA-related Requirements

Applicants **must demonstrate a direct and substantive relevance to the Cyber Resilience Act (CRA) scope**. This Open Call is addressed to business activities related to the development, manufacturing, import, or distribution of products with digital elements within the CRA scope, including their qualifying remote data processing solutions.

Applicants must operate in a sector or have business activity that reasonably falls, may fall or will fall within the CRA scope and regulatory framework or substantiate planned activities involving identifiable in-scope products. Furthermore, only Projects aimed at achieving compliance with the CRA will be accepted.

The CRA-related requirements must be clearly demonstrated during the drafting of the Proposal, by defining the operational context of the company in which the Project will be developed. The evaluation will focus on whether the current or future activities carried out by the company are expected to fall within the scope of the CRA. Applicants must clearly identify in their Proposal which products with digital elements, including qualifying remote data processing solutions, fall or will fall within the CRA scope to simplify the identification of their classification under the CRA and Implementing Regulation (EU) 2025/2392, taking account of Commission guidance.

In addition, the evaluation of the CRA-related requirements will take into account whether the proposed Project will effectively help the company to achieve, or move closer to, compliance with the CRA. **See *ANNEX 2-CRA Scope & Eligible Activities, Services and Goods* for further reference.**

Verification of CRA-related requirements will be part of the formal assessment carried out by designated SECURE Consortium partners.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

PROPOSAL & PROJECT SUBMISSION PROCESS

The submission and implementation stages are organised into the following phases:

STAGE 1 – Registration & Proposal Submission

During this stage, the Applicant will use the platform to enter company data and submit the project for which funding is requested. At the end of the submission, both eligibility and technical evaluations will be carried out.

PHASE 1
Registration & Company Documentation Upload

PHASE 2
Proposal & Budget Drafting

- **Actor**: Applicants
- **Available Time**: Call open for 2,5 Months
- **Applicants To Dos**: Document Upload & Draft

PHASE 3
Proposal Evaluation

- **Actor**: SECURE, Ev.Co., NCCs
- **Available Time**: Max. 4 Months
- **Applicants To Dos**: Platform & Email Monitoring

PHASE 4
Sub-Grant Agreement Signing

- **Actor**: Applicants
- **Available Time**: Max. 1,5 Months
- **Applicants To Dos**: Sign & Submit Sub-GA

STAGE 2 – Project implementation & Tech. Report

This stage will apply only to Applicants whose Proposals have been evaluated as fundable. Applicants will have 6 months to implement the project and complete their Technical Reports. Implemented Projects will then be funded.

PHASE 5
Initial CRA Maturity Assessment

- **Actor**: Applicants
- **Available Time**: Max. 6 Months
- **Applicants To Dos**: CRA Maturity Assessment

PHASE 6
Implementation & Technical Report

- **Actor**: Applicants
- **Available Time**: Max. 6 Months
- **ApplicantsTo Dos**: Implement Project & Report

PHASE 7
Implementation Assessment, Payment & Attestation

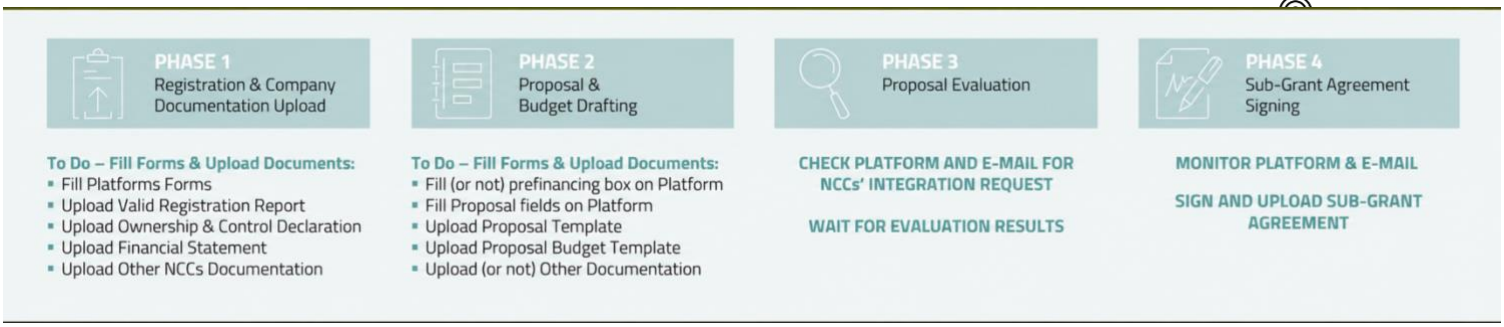
- **Actor**: SECURE & Ev.Co.
- **Available Time**: Max. 4 Months
- **Applicants To Dos**: Platform & Email Monitoring

***ICON LEGEND**: The following icons will be used to ease the identification of the types of Applicants activities*



3. STAGE 1 - Registration & Proposal submission process

The main phases of the registration and Proposal submission process are described below[2].



3.1. PHASE 1 – Registration & Company Documentation Upload

The Applicant accesses the SECURE Open Call platform through the official SECURE website, using the dedicated link that redirects to a registration panel requiring the creation of the Applicant account. Once logged in, Applicants will be required to complete the eligibility checklist, as outlined in Chapter 2.1. Upon the completion of the checklist, the platform will automatically generate the Applicant Declaration Document, which must be downloaded and signed by the company's legal representative using a **qualified electronic signature in PAdES format**. The digitally signed document must then be uploaded back to the platform in the designated field.

In addition, the other platform requests will have to be filled out. The Applicant will be required to:

- Obtain the **Valid Registration Report[3] (or equivalent documentation) with company good standing statement** from the Chamber of Commerce or another competent authority of their respective Member State and upload it on the platform. Together with the Registration Report the following evidence must be included:
    - Proof of indirect shareholders/owners
    - An ownership structure chart showing the complete ownership chain

      This evidence is important to ensure that the SME status is properly verified.
- Download, complete, and digitally sign the ***ANNEX 3-Ownership Control Declaration*** using a PAdES electronic signature, and re-upload the signed document to the platform.
- Upload the company's most recent **Financial Statement**, covering the latest closed financial year.
- Applicants must check whether their National Coordination Centre (**NCC**) requires **additional documentation** and, if requested, upload them on the platform.

2 All the deadlines described will be displayed on the platform and reminders will be sent via notifications and email.

3 The Registration Reports are issued by the relevant Chamber of Commerce or other competent authority. If the Registration Report does not contain all the necessary details listed above, the Applicant must request an integration from another competent national authority or relevant national database or provider and upload it on the platform.

Communications, Timing and Deadlines		
Action	**From**	**Until**
CALL PUBLICATION	**1/10/2026**	**29/01/2027**
Eligibility documentation submission *Uploading of Eligibility Documentation*	the publication date of the Call	the closing date of the Call

IMPORTANT NOTES

- *It is not necessary to have completed the upload of the eligibility documentation to start uploading the documents related to the Proposal.*
- *Once the requested documentation has been uploaded, modifications will be possible only until the final submission is completed (the action must be confirmed through the dedicated button available on the platform).*
- *Submissions must be completed by the closing date of the Call. After the submission of registration data and eligibility documents,* ***no further changes will be possible*** *through the platform, except in cases of explicit requests from the NCC (see section "Company eligibility Evaluation" of the chapter 3.3 "Proposal Evaluation").*



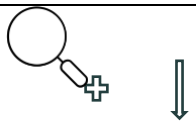
3.2. PHASE 2 – Proposal & Budget drafting

All forms and templates are available for download directly from the SECURE Open Call platform.
The process includes the following steps:

- **Proposal drafting**: Applicants must download the official Proposal Template from the dedicated link on the platform, complete all the required sections, and upload the document. If necessary, additional supporting documents may be uploaded as annexes to complement the Proposal. Applicants are requested not to exceed the text limits specified in the Project Proposal Template. Any text exceeding these limits will not be considered during the evaluation.
- **Budget preparation**: Applicants must complete the ***ANNEX 1.3-Proposal Budget Template***, available in Excel format, in line with the instruction included in the file. Further instructions for completing the Budget Template are provided in the ***ANNEX 1.2-Proposal Budget Guidelines***. After completing the budget, the file must be uploaded on the platform. All cost items indicated in the budget must be directly linked to the tasks and/or deliverables described in the Technical Proposal. Costs must be justified and the underlying assumptions clearly explained, avoiding both overestimation and underestimation of the resources required.
- **Pre-financing request**: After entering the Project budget on the platform, the Applicant may request pre-financing by selecting the appropriate option in the dedicated section of the platform.
- **Final review and submission**: Before confirming submission, Applicants should carefully review all information and uploaded files. Once the final submission button has been clicked, no further changes can be made through the platform.

Communications, Timing and Deadlines		
Action	**From**	**Until**
Proposal and Budget documentation submission *Uploading of Proposal and Budget*	the publication date of the Call	the closing date of the Call

IMPORTANT NOTES
• *Once the requested documentation has been uploaded, modifications will be possible only until the final submission is completed (the action must be confirmed through the dedicated button available on the platform).* • *Submissions must be completed by the closing date of the Call. After the submission of Proposal and Budget documentation,* ***no further changes will be possible*** *through the platform.*



3.3. PHASE 3 – Proposal Evaluation

Once the Proposal and budget documentation have been submitted, the application will enter the evaluation phase. In this phase, no action will be required from the Applicant unless otherwise specified. The evaluation phase is structured in three different levels:

a. Formal Evaluation
b. Technical Evaluation
c. Company Eligibility Evaluation



3.3.1. Formal Evaluation

This phase is conducted by Cyber 4.0, a partner of the SECURE Project and manager of the call.
During this stage, it will be verified that all CRA related requirements are fulfilled (see Chapter 2, Section 2.2), and that the activities described in the Proposal, for which funding is requested, fall within the scope of fundable activities outlined in the Call (see ***ANNEX 2-CRA Scope & Eligible Activities, Services and Goods***) The abstract and initial chapters of the Proposal will be examined to assess the Applicant's compliance with the required criteria.

3.3.2. Technical Evaluation

A **technical evaluation** will be carried out by an Evaluation Committee, composed of highly qualified cybersecurity and CRA experts from SECURE Project partners, assessing the quality of the proposed Project. Each Proposal will be evaluated by three evaluators and scored based on the evaluation criteria described in **Appendix B** of this document. At the end of the evaluation, a ranking of the Proposals will be created based on the scores achieved. Proposals that do not reach the minimum required score will be excluded from funding.
Before the technical evaluation begins, Cyber 4.0 shall carry out a **preliminary check** of the Proposals to identify any obvious clerical errors. Where such errors are identified, Cyber 4.0 shall notify the Applicant concerned, specifying the errors to be corrected and setting a deadline for the submission of a corrected version of the Proposal. The Applicant shall submit the corrected Proposal within the deadline specified in the notice.
Cyber 4.0 shall keep a record of the errors identified, the notices issued and the corresponding responses received.

For the purposes of these Guidelines, an «obvious clerical error» means a readily identifiable error, omission or inconsistency in the Proposal or its supporting documents (including minor omissions, easily recognisable textual errors, contradictory information, calculation errors, or incorrect entries or selections in an application form, and formal or technical irregularities relating to electronic signatures). Any correction of an error shall not result in a substantive amendment to the Proposal or confer an undue advantage on the Applicant.

The Evaluation Committee may request clarifications about the content of the Proposal, exclusively via email. The results of the technical evaluation will only be available if the applicant also passes the Company eligibility evaluation. At this stage, no notification will be sent to the Applicant through the Platform.

3.3.3. Company Eligibility Evaluation



The last evaluation phase is conducted by the National Coordination Centre (NCC) of the Member State where the Applicant is legally established, as declared by the Applicant itself in the relevant application form. Its purpose is to verify compliance with all Company Eligibility Requirements specified in the call. During this phase, NCCs may request additional documentation. In this case, the Applicant may log back into the platform to complete unlocked fields or upload the requested documents.
Any request of additional documentation will be communicated to the Applicant via notifications on the Platform and by email sent to the address provided during registration.
Once the Company eligibility evaluation has been completed the Applicant will receive a specific notification reporting one of four possible outcomes:

- Approval of company eligibility (valid only if the company also passed the technical evaluation).
- Request for integration.
- Rejection due to company ineligibility.
- Rejection due to lack of evaluation by the NCC (if the NCC has not completed the evaluation within the established deadlines or has not formally joined the verification process – see Section 2.1).

Successful completion of the company eligibility verification does not guarantee that the proposed Project will receive funding.
A list of National Coordination Centres is available at: https://cybersecurity-centre.europa.eu/nccs_en.

3.3.4. Eligibility & Technical evaluation final results



Applicants that successfully pass the formal eligibility evaluation, the technical evaluation and the company eligibility evaluation will receive an official notification via the Platform and by email, including the results of the Technical Evaluation. Applicants that do not successfully pass the company eligibility evaluation will not receive the Technical Evaluation results. Once all three evaluation phases have been completed, a list of eligible Proposals will be prepared.
The Applicant Company will receive a specific notification containing the final result of their Proposal's evaluation. The following scenarios may occur:

- **Proposals admitted for funding**: Proposals admitted for funding will be invited via notification on the platform to proceed with the signing of the sub-grant agreement
- **Proposals eligible for funding but not admitted due to budget constraints**: Proposals that have successfully passed the technical evaluation but cannot be funded due to insufficient budget will receive a notification via the platform.
- **Proposals not eligible for funding**: Proposals that did not achieve the minimum required score for funding will receive a rejection notification.

Communications, Timing and Deadlines		
Action	**From**	**Until**
Evaluation Result Notification (Admission/Rejection)	the closing date of the Call	Approx. 3 months from the closing date of the Call

3.4. PHASE 4 – Sub-Grant Agreement (Sub-GA) Signing



If the Proposal successfully passes all evaluation stages, the Applicant will be required to sign the Sub-Grant Agreement. During this phase, the following procedure shall apply:

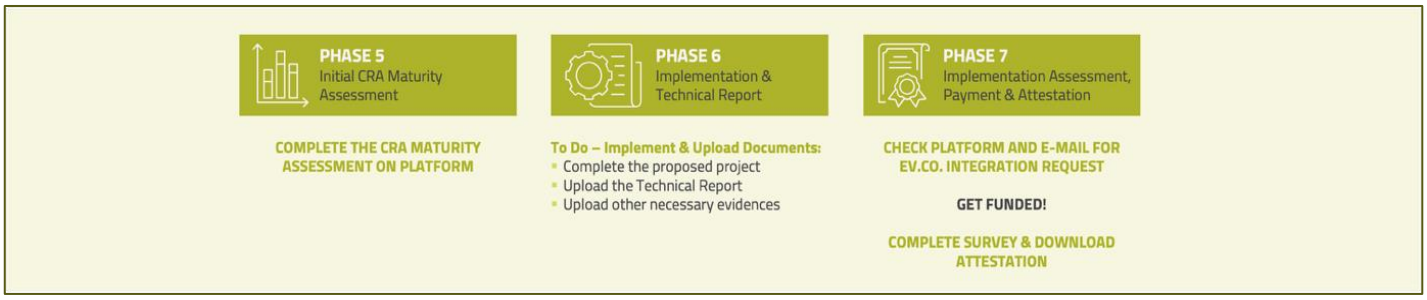
- Proposal fully approved: the Proposal has achieved the minimum technical score threshold required to be considered eligible for funding. The company will be admitted to the "Project Delivery" Phase and will receive funding after the Sub-GA signing. The Applicant will receive a notification via email and through the platform, with the Sub-GA Annex attached. This document must be signed by the Applicant's legal representative using a qualified electronic signature (QES), in PAdES format, and uploaded in the designated area of the platform.

Following the signature of the Sub-GA, the Sub-GA will be countersigned by the Project Coordinator. If the Applicant requested pre-financing during Phase 2, the pre-financing amount will be disbursed either at the same time as, or within a few days after, the countersignature of the Sub-GA.

Communications, Timing and Deadlines		
Action	**From**	**Until**
Sub-Grant Signing deadline	The receipt of the notification approval	Approx. 1 month from the receipt of the approval notification

4. STAGE 2 - Project Implementation and Technical Report Submission Process

The implementation stage consists of the following 3 main phases:



Once the Sub-GA has been signed, the proposed Project will be officially selected for funding. The Applicant Companies will therefore be formally recognized as **Beneficiary Companies**. From the moment of signature of the Sub-GA, the Beneficiary Company (Beneficiary) may start the Project implementation stage. At the Beneficiaries' discretion, implementation activities may also begin before receiving the countersigned Sub-GA. However, only the costs actually incurred and supported during the official Project implementation period (i.e., after the signature of the Sub-Grant Agreement) are considered eligible.

4.1. PHASE 5 – Initial CRA Maturity Assessment

Once the Grant Agreement has been signed, a page will be displayed on the platform containing a link to a CRA Maturity Assessment survey. This consists of a short questionnaire that the Beneficiaries must download and complete following the provided instructions. Once completed, the CRA Maturity Assessment must be signed using a qualified electronic signature in PAdES format and uploaded to the designated section of the platform.

Completion of the CRA Maturity Assessment is mandatory, and the uploaded template will be considered a compulsory annex to the Technical Report to be submitted later. Until the CRA Maturity Assessment has been uploaded to the platform, the Beneficiaries will not be allowed to upload the Technical Report. This means that if the **CRA Maturity Assessment is not completed within the implementation period, the Project will be considered NOT IMPLEMENTED and NOT ELIGIBLE FOR FUNDING.**

Communications, Timing and Deadlines		
Action	**From**	**Until**
Initial CRA Maturity Assessment completion	signing of Sub-GA	upload of the Technical Report[4]

IMPORTANT NOTES
Until the CRA Maturity Assessment is completed, it will not be possible to upload the Technical Report. This does not prevent the Beneficiary from starting the Project implementation activities or from drafting the Technical Report offline, as the template will be made available immediately.

[4] For the completion of the Risk Assessment, Project implementation, and uploading of the Technical Report, the Beneficiaries will have 180 days from the signing of the Sub-GA)-.

4.2. PHASE 6 – Implementation & Technical Report

The Project implementation may begin once the signed Sub-GA has been uploaded. During this phase, the Beneficiary must carry out the activities described in the Proposal while maintaining all documentation necessary to verify the implementation process. The results shall be reported through the completion and upload of the ***ANNEX 6-Technical Report Template.*** This report must include specific references to the achievement of the KPIs declared in the Proposal and the completion of the Deliverables. In addition to the description provided in the Technical Report, all supporting evidence defined in the Proposal must be prepared. In particular, the company will be required to upload documents proving the completion of specific Deliverables that cannot be integrated into the Technical Report (e.g., technical Deliverables, source code, VA outputs, network mappings, multimedia materials such as photos/audio/video, etc.). These documents must provide clear evidence that the declared KPIs have been met. Beneficiaries will not be requested to present financial reports or supporting documents to demonstrate the actual costs incurred. Further guidance and recommendations are provided in ***ANNEX 2-CRA Scope & Eligible Activities, Services and Goods***.

Communications, Timing and Deadlines		
Action	**From**	**Until (calendar days)**
Technical Report, Deliverables & Evidence Upload *Uploads are enabled only after the completion of the Initial CRA Maturity Assessment*	the signing of Sub-GA	180 days from the signing of the Sub-GA

IMPORTANT NOTES

- *During the 180-day implementation period, beneficiaries are required to complete both the full implementation of the Project and the drafting of the Technical Report. Submissions after the deadline will not be accepted, unless otherwise requested by the Evaluation Committee.*
- *Except for specific modification requests issued by the Evaluation Committee (see the next section), once the Technical Report has been submitted, no further changes to the uploaded material will be allowed.*
- *The evaluation of the Deliverables by the Evaluation Committee will take place only after the 180-day implementation period has ended. Early submission of the Technical Report is permitted; however, it will not result in early payment.*

4.3. PHASE 7 – Implementation Assessment, Payment & Attestation

The following steps will take place after the submission of the Technical Report together with the related annexes and evidence:

- **Implementation Evaluation**: The Technical Evaluation Committee will assess whether the Project has been effectively implemented. This assessment will be based on the details provided in the Technical Report and on the annexed evidence. The Committee's analysis will focus on verifying the achievement of the KPIs declared during the Proposal stage.

  During this evaluation, the Committee may request additional documentation or amendments to the submitted material. In such cases, the company will be enabled to update or integrate the uploaded documentation. Further information on Implementation Evaluation is provided in the **Appendix C.**
- **Balance Payment**: The balance payment will be made based on the Committee's evaluation (see **Appendix C**). Three possible scenarios may occur:

- Objectives Fully Achieved – Full Balance Payment: If the Evaluation Committee concludes that the Project has been 100% implemented, the company will receive the full balance corresponding to the total grant amount specified in the Sub-GA. If a pre-financing payment has already been made, the balance will correspond to the difference between the total grant and the amount already disbursed as pre-financing.
- Objectives Partially Achieved – Partial Balance Payment: If the Evaluation Committee determines that the Project has only been partially implemented, it will indicate a percentage of completion based on the KPIs achieved. The grant amount will be recalculated accordingly (e.g., if the requested funding was EUR10,000 but the Committee determines that only 60% of the Project was completed, the company will receive EUR 6,000).
- Objectives Not Achieved – No Balance Payment: If the Evaluation Committee determines that the Project has not been implemented at all, the balance payment will not be made.

- **Attestation of Project Completion**: The Beneficiary is encouraged to communicate about the Project and its successful completion through its own dissemination channels. To demonstrate successful implementation, Beneficiaries may use the "Formal Attestation of Project Completion," which can be downloaded from the platform after completing two mandatory surveys: Final CRA Maturity Assessment and other SECURE Project-related surveys.

Communications, Timing and Deadlines		
Action	**From**	**Until**
Technical Report Assessment by the Eval. Committee and Balance Payment	the day of the Technical Report upload	Approx. 2 months
Attestation and Survey Upload	the day of the Technical Report upload	the closure of the SECURE Project

IMPORTANT NOTES

- *The Evaluation Committee can request amendments to the Technical Report and Evidence*
- *For further information on the possible outcomes and consequences of the Implementation Assessment consult* ***Appendix C****.*

5. Communications and Information

- **FAQ**: https://secure4sme.eu/
- **CONTACTS**:
  - Link: https://secure4sme.eu/
  - submission-support@secure4sme.eu

6. Mandatory Annexes and Supporting Documents

Proposal Mandatory Annexes:

- ANNEX 1.1-Proposal Template – Call 2
- ANNEX 1.3-Proposal Budget Template – Call 2
- ANNEX 3-Ownership Control Declaration – Call 2
- ANNEX 4-Valid Registration Report (or equivalent documentation) with company good standing statement (provided by National Chamber of Commerce or other competent authority)
- ANNEX 4.1-Company Financial Statement (to be drafted autonomously)

Implementation Mandatory Annexes:

- ANNEX 5-Sub-Grant Agreement - SAMPLE – Call 2
- ANNEX 6-Technical Report Template – Call 2

Support Documents:

- ANNEX 1.2-Proposal Budget Guidelines – Call 2
- ANNEX 2-CRA Scope & Eligible Activities, Services and Goods – Call 2
- ANNEX 7-Formal Attestation of Project Completion – Call 2

Appendix A – Company Eligibility Criteria

A. Individual Entities

Only individual legal entities (private bodies) are eligible to apply to the Open Call. Each application must be submitted by a single organization acting independently in its own name. Consortia, business networks, or joint applications are explicitly excluded. (this requirement ensures that the Applicant assumes full responsibility for Project implementation and compliance with the grant agreement). Although consortia are not considered eligible, subcontracting remains an eligible cost. This means that applicant companies are allowed to use co-funding to cover professional services provided by third-party suppliers (such as consultants or service providers). The rules governing subcontracting are defined in ***Annex 1.2 – Proposal Budget Guidelines***.

Specific Cases:

- **Natural persons** — Natural persons are NOT eligible (except for self-employed persons, i.e. sole traders, where the company does not have legal personality separate from that of the natural person).
- **International organisations** — International organisations are not eligible.
- **Entities without legal personality** — Entities which do not have legal personality under their national law are not eligible.
- **EU bodies** — EU bodies can NOT participate in the Open Call.
- **Associations and interest groupings** — Entities composed of members may participate as 'sole beneficiaries'. Please note that Projects shall not be submitted jointly by an association and one or more of its members. Association members may participate individually by submitting their own independent Project Proposals as individual entities, provided they meet the eligibility requirements described in this call.
- **EU restrictive measures** — Special rules apply for certain entities (e.g. entities subject to EU restrictive measures under Article 29 of the Treaty on the European Union (TEU) and Article 215 of the Treaty on the Functioning of the EU (TFEU)[5] and entities covered by Commission Guidelines No 2013/C 205/059). Such entities are not eligible to participate in any capacity, including as beneficiaries, affiliated entities, associated partners, subcontractors or recipients of financial support to third parties (if any).

Following the Council Implementing Decision (EU) 2022/2506, as of 15th December 2022, no legal commitments (including the grant agreement itself as well as subcontracts, purchase contracts, financial support to third parties etc.) can be signed with Hungarian public interest trusts established under Hungarian Act IX of 2021 or any entity they maintain.

B. mSMEs definition

Only micro, small and medium enterprises (mSMEs) are eligible for funding. The criteria for qualifying as an SME are defined according to the EU Commission Recommendation 2003/361/EC [6](see also: official "*User groups*

5 Please note that the EU Official Journal contains the official list and, in case of conflict, its content prevails over that of the EU Sanctions Map.

6 See CRA Article 3(19) and the Annex to Commission Recommendation 2003/361/EC for the applicable SME definition; accounting thresholds under Directive (EU) 2023/2775 do not replace that definition.

Guide to the SME definition"[7]). Applicants must declare their SME status in the **Applicant Declaration Form** (available only on the platform, during the completion of the registration process) **and in the *ANNEX 3- Ownership Control Declaration***, which will be verified during the eligibility evaluation process.
According to the Commission Recommendation 2003/361/EC, and as recalled in the SECURE Grant Agreement, mSMEs are enterprises:

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

Article 3 of the Annex to Commission Recommendation 2003/361/EC, distinguishes between different levels of affiliation affecting an mSME's eligibility depending on how the financial amounts and staff headcount shall be calculated.

- Autonomous enterprises are those that are not classified as partner or linked enterprises.
- Partner enterprises are those in which one company, either alone or together with linked enterprises, holds 25% or more of the capital or voting rights.
- Linked enterprises exist when one enterprise:
    - Has majority voting rights in another;
    - Can appoint or remove the majority of the administrative, management, or supervisory body;
    - Exercises dominant influence through contractual or statutory means;
    - Controls, alone or with others, a majority of voting rights in another enterprise

The Applicant shall qualify as a micro, small or medium-sized enterprise (mSME), as defined in Commission Recommendation 2003/361/EC, and shall maintain such status and continue to meet all other applicable eligibility requirements. Any subsequent loss of such status, as determined in accordance with the criteria set out in Commission Recommendation 2003/361/EC, or failure to meet any other applicable eligibility requirement shall render the Applicant ineligible for funding.

C. Geographical Eligibility

Only individual mSMEs **legally established** in an eligible Country may participate in this Open Call.
For the purposes of this Open Call, eligible Countries are:

- EU Member States (including overseas countries and territories - OCTs)
- EEA countries (Norway, Iceland, Liechtenstein)

To be eligible Applicants must cumulatively meet the following requirements:

- be legally established in one of the eligible Countries and provide evidence of their legal establishment;
- be entities whose Ultimate Beneficial Owner is a citizen of one of the eligible Countries;
- carry out Project activities in one of the eligible Countries;
- comply with the applicable ownership and control requirements pursuant to Article 12(5) of Regulation (EU) 2021/694 and Article 136(3)(a) of Regulation (EU, Euratom) 2024/2509. Only

7 https://op.europa.eu/en/publication-detail/-/publication/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1

entities controlled from EU Member States and the specified eligible non-EU countries (EEA Countries) may participate in this Open Call. The ownership and control of the Applicant shall be assessed in accordance with the *European Commission's guidance on participation in EU calls with ownership and control restrictions* available at the time of the assessment.

D. Legal and ethical requirements and exclusions

Applicants must comply with all relevant legal, ethical, and financial obligations under both national and EU law. To access the funding, the Applicant must declare, through the dedicated form on the platform, that none of the following possible grounds for exclusion apply:

In accordance with Articles 137 and 138 of the Financial Regulation, Applicants will be excluded from participation if they:

- Have been convicted by final judgment of:
    - Fraud, within the meaning of Article 3 of the Directive (UE) 2017/1371 of the EU Parliament and of the Council;
    - Corruption, as defined in Article 4 of the Directive UE) 2017/1371 of the EU Parliament and of the Council;
    - Participation in a criminal organisation, as defined in Article 2 of Council Framework Decision 2008/841/JHA;
    - Money laundering or terrorist financing, as defined in Article 1 of the Directive (EU) 2015/849;
    - Terrorist offences or offences linked to terrorist activities, as defined in Articles 3 to 12 of Directive (EU) 2017/541 of the EU Parliament and of the Council, or inciting, aiding, abetting or attempting to commit such offences, as referred to in Article 14 of that Directive;
    - Child labour or other offences concerning trafficking in human beings, as referred to in Article 2 of Directive (EU) 2011/36 of the European Parliament and of the Council.
- Have shown significant deficiencies in complying with the main obligations in the performance of a contract financed by the EU budget, resulting in early termination, damages, or comparable sanctions;
- Have been found guilty of grave professional misconduct proven by any means which the contracting authority can justify;
- Have been declared bankrupt, are being wound up, have their affairs administered by the courts, have entered into an arrangement with creditors, or are in any analogous situation arising from a similar procedure;
- Have been found in one of the Exclusion Criteria set out by Art. 138 of the Financial Regulation;
- Are subject to an administrative penalty under Article 140 of the Financial Regulation;
- Qualify as an "enterprise in difficulty" in accordance with Article 2(18) of Commission Regulation No 651/2014;
- Are excluded from receiving EU funding under national or EU law, or by a decision of a national or EU authority.

Applicants must confirm compliance with these requirements through the **Applicant Declaration Form**, which must be duly completed, signed, and submitted together with the Proposal. Supporting evidence may be requested during the eligibility verification phase.

E. Double funding exclusion

Applicants must ensure that the proposed Project is **not subject to double funding**. The fundamental principle underpinning the rules for public expenditure in the EU states that no costs for the same activity can be funded twice from the EU budget, as defined in Regulation (EU, Euratom) 2024/2509, Art. 194.

APPENDIX B - Proposal Technical Evaluation

A. Evaluation Committee

The objective of the Evaluation Committee (Ev.Co.) is to provide a technical assessment and evaluation of the Proposals and Project Technical Report and evidence submitted by the Applicant Companies.
As defined in the following sections, the Ev.Co. has 2 mains roles:

1. Assigning a score to each Proposal to determine a ranking of the Proposals and the Projects eligibility for funding.
2. Evaluating whether the funded Projects have been successfully completed through the analysis of the Deliverables.

The Ev.Co. for this Open Call is appointed by SECURE Consortium Partners that will select individual experts from the staff of the partner organizations. Specifically, each Partner may propose a single Committee member chosen from its own staff, provided they meet the professional and educational requirements necessary to perform the assessments.
The Ev.Co. will consist of a minimum of 21 members (one per SECURE Partner).
Evaluation Committee Members will be selected from the pool of cybersecurity and compliance experts.
For the evaluation and scoring of the Proposals and the analysis and evaluation of the Deliverables, the Ev.Co. will schedule several "consensus meetings", which must be convened by the Committee Chair or their Deputies.

B. Proposal Evaluation Criteria

Proposals will be assessed according to the following awarding criteria:

1. **Excellence and relevance**

This criterion focuses on the quality, clarity, and credibility of the proposed action in relation to the objectives of the Cyber Resilience Act (CRA). Evaluators will consider:

- **Relevance to EU cybersecurity goals on CRA:** the degree to which the Project activities fall within the scope of the CRA. The evaluation will consider the level of detail with which the Applicant describes the compliance gap that needs to be addressed to align with the CRA requirements, as well as the extent to which the proposed Project will be able to bridge this gap. The evaluation will consider also how effective the proposed activities are in achieving an adequate level of compliance with the CRA.
- **Project objectives and methodology:** the degree to which Project objectives are consistent and realistic. The evaluation will consider purchased services and goods, technological and human resources allocated to the Project, business segment involved in the compliance process (e.g., internal departments, ICT, OT, IoT infrastructures), relevant improvements of the Applicant's infrastructures (upgrading, replacement, new solutions adoption) or processes.
- **Resources and capabilities:** Proof of sufficient resources and personnel to execute the proposed activities. If additional tools or specialised equipment are required, Applicants should outline acquisition plans.

2. Impact and Clarity

This criterion evaluates the expected benefits of the Project and the clarity of the whole Proposal, with a direct link to the CRA. Evaluators will consider:

- **Expected outcomes for the mSME:** the degree to which concrete benefits for Applicant mSME are achieved. Evaluation will assess the following possible achievements: the increase of compliance level with CRA, the alignment with other regulatory frameworks, the improved competitiveness in European and international markets, the enhancement of cybersecurity posture, the improvement of operational resilience, and the efficiency of internal processes and procedures.
- **Clarity of description:** The level of clarity of the descriptions provided within the whole Proposal and the consistency of short and long-term advantages for both the company and its stakeholders compared to the effective actions described.
- **Indicators and KPIs to measure success:** The degree to which KPIs are measurable and verifiable to monitor progress and assess results. Evaluation will assess also the consistency of KPIs in relation to the described objectives.

3. Implementation

This criterion assesses the feasibility and practicality of the Project plan and the quality of the Proposal Implementation section. Evaluators will consider:

- **Work Packages (WP):** the degree to which the description of the action is properly structured into Work Packages, defining clear objectives, tasks, achievable Milestones, and measurable Deliverables. Tasks should include defined durations; Milestones should be linked to deadlines; and Deliverables should consist of tangible outputs (e.g. reports, technical documents, software components). Each Deliverable must include KPIs and supporting evidence. The maximum Project duration is 6 months, and at least one Work Package (WP1) is mandatory, while there should be a maximum of 3 WPs.
- **Deliverables, evidence and cost consistency**: the clarity degree to which Deliverables, evidence and their alignment with the declared KPIs are described. The evaluation will consider how well the proposed Deliverables and supporting evidence can demonstrate the achievement of the stated KPIs. In particular, the assessors will consider how demonstrable the KPIs will be during the Technical Report evaluation phase, based on the contents provided through Deliverables and supporting evidence. This assessment will compare the Project Deliverables with the indicated effort in terms of costs, implementation times, deadlines, planned activities, and the personnel or experts involved to assess the consistency and the feasibility of the Project. Also, a transparent and realistic breakdown of costs, with a maximum reimbursable cost of EUR 30,000 will be considered. The Proposal must include credible Deliverables aligned with budget estimates in terms of person-months, technologies, and other required resources.
- **References to other Digital European Program CRA-related projects:** the extent to which the implementation of the proposed Project involves the direct use of tools, activities, goods, or services promoted by other DEP CRA related projects, either completed or currently ongoing. This parameter considers direct references to other DEP Projects, rewarding Proposals that rely most heavily on tools or outputs developed by other European Projects focusing on the CRA implementation to achieve their objectives (e.g.: conformity, risk and maturity assessment tools; official guidelines and standards; auto-assessment tools and models).

C. Proposal Scoring

1. Individual Evaluation

Each evaluator, based on the defined criteria, will assign an individual evaluation, which will be documented in an Individual Report to be presented during the consensus meetings of the Ev.Co.

Within individual evaluations, evaluators will score each award criterion on a scale from 0 to 5:

- **0 =** Proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.
- **1 =** Poor – criterion is inadequately addressed or there are serious inherent weaknesses.
- **2 =** Fair – Proposal broadly addresses the criterion, but there are significant weaknesses.
- **3 =** Good – Proposal addresses the criterion well, but shortcomings are present.
- **4 =** Very good – Proposal addresses the criterion very well, with only minor shortcomings.
- **5 =** Excellent – Proposal successfully addresses all relevant aspects of the criterion; shortcomings are negligible.

2. Consensus Evaluation

Each evaluator will present to the Evaluation Committee Consensus Meetings the Individual Evaluation Score. The final score for each criterion will be the sum of the evaluators' scores, **with a maximum score of 15 points for each criterion**. The average results will always be rounded using standard rounding to the nearest integer. The overall final score will be the weighted average of all criteria, with a **maximum total score of 15**.

For the calculation of the weighted average of the final score, considering the relevance of each section of the Proposal template to which the described criteria refer, the following weights will be applied to each parameter:

- Quality & Relevance = 1.5
- Impact & Clarity = 1.5
- Implementation = 1

Technical Evaluation exclusions will be based on the following threshold:

- **Minimum threshold per criterion:** All Proposals with a score below **10 (<10)** in two or more criteria will be excluded from financing.
- **Minimum overall threshold:** All Proposals with a total score below **10 (<10)** will be excluded.

If there is a discrepancy of 5 points or more between evaluators on two or more criteria, an additional evaluator will be involved to provide an additional assessment. The scores provided by all evaluators will then be used to calculate a new weighted average for the final score.

Evaluators / Criteria	Evaluator 1	Evaluator 2	Evaluator 3	ROUNDED SUM	WEIGHTS
Quality & Relevance	3	4	4	11	**1,5**
Impact & Clarity	3	2	2	7	**1,5**
Implementation	5	5	4	14	**1**
ROUNDED WEIGHTED AVERAGE				10	

Consensus Scoring – Fundable Proposal Example

Tie-breaking rules

In case of a tie, the final ranking will be determined based on the submission date and time of the Proposal on the platform. Specifically, in the event of a tie, Proposals submitted earlier will be ranked higher than those submitted later. Amendment periods will not be considered for this calculation.

APPENDIX C - Implementation Assessment

A. Project Implementation & Technical Report Assessment

The evaluation of the Project Implementation and Technical Report will be carried out following the submission of the technical material after the 6-month period that Applicants have for implementing the proposed Project. The evaluation will aim to verify that the proposed activities have been successfully implemented. Evaluators will not be required to assign scores but only to confirm that what was declared during the Proposal phase has been fulfilled. Specifically, the following aspects will be assessed:

- **Deliverables:** The Deliverables have been completed and are fully verifiable based on what is described in the Technical Report and supported by the available evidence.
- **Milestones:** Milestones have been reached and are supported by clear and reliable evidence.
- **KPIs:** KPIs have been achieved and are clearly demonstrated through the evidence, Milestones, and deliverables.

The Technical Report and evidence will be evaluated by the same number of individual evaluators of the Proposal evaluation. The Project's fundability will be determined by majority vote during the consensus meeting. In this phase, Committee members are divided into groups of 3, with each evaluator providing an **individual judgement** of the Project implementation.

B. Implementation Evaluation Outcomes

1. Individual Assessment

Each evaluator can assign one of three possible judgments:

- Objectives Fully Achieved (Full Balance Payment)
- Objectives Partially Achieved (Partial Balance Payment)
- Objectives Not Achieved (No Balance Payment)

2. Consensus Meeting

If all three evaluators provide different judgments, a fourth evaluator will be called to give a decisive opinion for the consensus evaluation. The final Project evaluation is determined by the majority of votes among the three (or four) evaluators.

3. Evaluation outcomes and Financial Implications

Depending on the majority decision, there are three possible outcomes:

- Objectives Fully Achieved – If the Evaluation Committee concludes that all Project objectives and KPIs have been achieved, the company will receive the full balance corresponding to the total grant amount specified in the Sub-GA.
- Objectives Partially Achieved – If the Evaluation Committee determines that the objectives have only been partially achieved, it will indicate a percentage of completion based on the KPIs met. The grant amount will be recalculated accordingly. In this case, the evaluators forming the majority must determine and justify the percentage of Project completion based on the quantification of Deliverables, Milestones, and KPIs actually achieved compared to those declared in the Proposal. This percentage is then applied to the total Project balance during the balance payment phase. Example: a Project requesting EUR 10,000 but judged 60% completed will receive EUR 6,000.

- Objectives Not Achieved – If the Evaluation Committee determines that the Project objectives and KPIs have not been achieved at all, no balance payment will be made, and the Beneficiary may be required to reimburse any advance payment received.

In the event that the objectives are not achieved or only partially achieved, or the project cannot be properly assessed due to missing or unusable documentation, the following measures apply:

- Failed Project: a Project will be considered "Failed" only if the Technical Report or the supporting documentation is not uploaded, if the uploaded documentation is empty or illegible. It is the responsibility of the Evaluation Committee to report to the company any uploading issues and allow the company to re-upload the materials within the timeframe available for amendments. If, even after the allowed amendment period, the Committee is not put in a position to review the Technical Report or supporting evidence, the Project will be deemed not implemented and the funding will not be disbursed.
- Prefinancing Return on Failed Projects: If, following the notification referred to in the preceding paragraph, the Beneficiary fails to respond within the specified deadline, the Project shall be deemed "Failed". Where the Beneficiary has already received pre-financing, the SECURE Project Coordinator may request repayment of the amounts already disbursed, in accordance with the Sub-GA;
- Prefinancing Return on partially implemented Projects: if a company whose Project is deemed "partially implemented" (objectives partially achieved) has received pre-financing exceeding the amount of funding effectively granted, following the budget reduction proposed by the Committee, the SECURE Project Coordinator shall have the right to request the return of the excess funds already disbursed.
- Prefinancing Return on Projects with Objectives Not Achieved: If a company whose Project is deemed "Objectives Not Achieved" has received pre-financing, the SECURE Project Coordinator shall have the right to request the return of the funds already disbursed.

Any non-compliance, including cases where the project objectives are not achieved in whole or in part, shall be addressed through formal written communications with the partners responsible for the relevant activities, in accordance with the Sub-GA.