SECURE
Cyber Resilience for SMEs

Second Info Day on the 1st SECURE Open Call

Agenda

10:00 – 10:10	**Welcome, introduction and overview of the agenda** *ACN & Cyber 4.0*
10:10 – 10:40	**FSTP: SECURE 1st Open Call – Application & Implementation Process** *Speaker: Alessandro Calabrese, Head of Advisory & Training (Cyber 4.0)*
10:40-10:50	**SECURE Open Platform – Registration & Proposal Submission** *Speaker: Alberto Garinei, CTO (Idea-Re)*
10:50 – 11:30	**Q&A & Open Discussion with Applicants**

Funded by the European Union

Table of Contents

INTRODUCTION

1. Secure Project Scope & Objectives (total budget & Partners)
2. 1st Open Call General Information (deadline & Grant)

ELIGIBILITY REQUIREMENTS

4. Call Eligibility Requirements
5. Company Eligibility Criteria
6. The role of the NCCs
7. Application & Implementation Stages on the SECURE online platform

APPLICATION & IMPLEMENTATION PROCESS

9. PHASE 1 - Registration & Company documentation upload
10. PHASE 2 - Proposal & Budget Drafting
11. PHASE 3 - Proposal Evaluation
12. Technical Evaluation Criteria
13. PHASE 4 - Results & Sub-Grant Signing
14. PHASE 4 – Sub Grant Signing & Material Errors Amending
15. STAGE 1 – Budget focus
16. STAGE 2 – Project Implementation & Technical Report
17. Documents and web references

Funded by the European Union

SECURE
Cyber Resilience for SMEs

Introduction

SECURE - Strengthening EU SMEs Cyber Resilience Project

SECURE
Cyber Resilience for SMEs

Coordinator:

- Agenzia per la Cybersicurezza Nazionale (ACN)

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).

Project Scope

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) -*** *Regulation (EU) 2024/2847*, through the launch of Open Calls for financial support.

Project Total Budget

EUR 16,5 Million

Number of Open Calls in the next years

At least 2

Target Applicant

EU and EEA Micro, Small and Medium Enterprises

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1st Open Call General Information

SECURE
Cyber Resilience for SMEs

Financial support for mSMEs to **co-finance mini-projects** (activities, goods and services) aimed at strengthening cyber resilience and achieve the compliance with the Cyber Resilience Act.

Open Call Operational Information

Call Launch Date
28/01/2026

Call Deadline
29/03/2026

Language
ENGLISH

Grant Type
LUMP SUM Funding
(no mandatory financial reporting)

Budget and Cofinancing

Call Total Budget
EUR 5,000,000

Projects Cofinancing Rate
50%

Prefinancing (optional)
Max. 40% of the grant

Maximum Grant
EUR 30,000

The Ceiling applies also to projects with total eligible costs higher than EUR 60.000

All Relevant Call Documents will be shared today on the website

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SECURE
Cyber Resilience for SMEs

Eligibility Requirements

Call Eligibility Requirements

SECURE
Cyber Resilience for SMEs

1. Company Eligibility Criteria

- The Applicant is an individual entity
- The Applicant is a mSME (*https://eur-lex.europa.eu/eli/reco/2003/361/oj/eng*)
- The Applicant is established in one of the eligible countries (EU + EEA)
- The applicant meets all the ethical and legal requirements (only self dec.)
- Absence of double funding (only self dec.)

2. CRA-Related Eligibility Criteria

- **Applicants CRA scope Requirements**: Applicants must operate in a sector or have business activity that falls within the CRA scope and regulatory framework or demonstrate willingness to do so
- **Eligible Activities**: only projects aimed at achieving compliance with CRA will be accepted

Who Can Apply? 1/3
Company Eligibility Criteria

SECURE
Cyber Resilience for SMEs

All eligibility criteria must be met to apply for the call

1

Individual Entities

Eligible Organizations

- Single organization with legal personality acting independently in its own name
- Self employed persons (i.e: sole traders)
- Associations and interest groupings with legal personality (only as sole beneficiaries)

Exclusions

- Consortia, business networks or joint applications
- Natural Persons (except for self-employed persons - i.e: sole traders)
- International Organizations
- Entities without a legal personality
- EU bodies
- Other special cases (see Annex 1)

2

mSMEs Definition

Enterprise category	Headcount: annual work unit (AWU)	Annual turnover	or	Annual balance sheet total
Medium-sized	< 250	≤ EUR 50 million	or	≤ EUR 43 million
Small	< 50	≤ EUR 10 million	or	≤ EUR 10 million
Micro	< 10	≤ EUR 2 million	or	≤ EUR 2 million

For Partner & Linked enterprise definition please visit: https://op.europa.eu/en/publication-detail/-/publication/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1

3

Geographical Eligibility

Company HQ or Branch for which the financing is requested & UBO Nationality shall be EU + EEA

4

Legal and ethical Requirements

e.g: no conviction by final judgment for fraud, corruption; no guilt of professional misconduct …

5

No Double Funding

Submitted project must not be subject to double funding

The role of National Cybersecurity Coordination Centres (NCC)

SECURE
Cyber Resilience for SMEs

What are NCCs?

NCCs are **public entities designated by each EU Member States + Norway and Iceland** established to strengthen research, innovation and industrial capabilities **in the field of cybersecurity**. E.g. they are responsible for:

- coordinating national activities with the European Cybersecurity Competence Centre (ECCC);
- promoting research excellence and industrial competitiveness across the Union;
- facilitating collaboration among industry, the public sector, academia and citizens;
- ***Facilitating access to EU funding opportunities to industry stakeholders.***

NCCs' roles and responsibilities are regulated under ***[ECCC] Regulation (EU) 2021/887***

Which is the role of the NCC during the SECURE Open Call

Within SECURE Project and during SECURE Open Calls NCCs **will carry out Companies Eligibility Checks and support enterprises during the application.**

Companies based in a Member State whose NCC does not support the SECURE Project First 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

How to make sure that the NCC representing my country will support the project?

Soon on SECURE website will be available a list of the nationalities of the supporting NCCs. Make sure to check the presence of your country.

How can I contact my NCC by my own?

Here's the public list of NCCs contact points:
https://cybersecurity-centre.europa.eu/nccs_en

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Who Can Apply? (2/3)
Applicants CRA-Related requirements

SECURE
Cyber Resilience for SMEs

Economic operators under CRA Scope

Manufacturers

Importers

Distributors

Open-source software stewards

OF

Products with digital elements (PDEs) – Focus of CRA Category within the first Open Call

Category	Brief Meaning	Compliance Procedure	Example Products
Default Products	Low-risk PDEs (~90% of total), general consumer or office devices	Internal self-assessment leading to an EU declaration of conformity	Standard printers, USB drives, office productivity software, smart speakers, connected light bulbs, fitness trackers

Based on the adoption of implementing acts by European Commission specifying technical descriptions of categories of products with digital elements, the next Open Calls will be focused also on:

- Important Products (Class I and II)
- Critical Products

ADMISSIBLE COMPANIES: the Applicant Company falls, may fall or will fall under the CRA Scope based on the CRA Regulation (Regulation-EU 2024/2847)

Who Can Apply? (3/3)
Eligible Activities & Other EU Projects

SECURE
Cyber Resilience for SMEs

Category 2: *CRA Cybersecurity Governance, Risk Management and Compliance Assessment – Modules 1, 2 and 3*

Category 3: *CRA requirements training*

Category 4: *CRA-related cybersecurity trainings*

Category 5: *Expertise support in the CRA conformity project execution*

Category 6: *Vulnerability tests*

Category 7: *Laboratory tests*

Category 8: *Penetration tests*

Category 10: *CRA self-assessment tool*

Category 11: *Software Development – Security by Design for CRA Products*

Category 12: *Business Continuity, Incident and Response Planning for CRA Products and Processes*

Category 13: *Supply Chain Risk & Security Assessment*

Category 14: *Data Protection & Privacy Compliance*

Category 16: *Monitoring, protection and prevention services and tools*

SECURE is building **synergies with other CRA implementation DEP projects**.
Tools developed under these linked projects will be made available to mSMEs to support eligible activities under the cascade funding scheme.

Category 1: Accredited trusted third-party audit with the CRA certificate

Category 9: CRA third-party assessment service

Category 15: CRA Regulatory Obligations and Documentation Support

→ **Out of Call 1 Scope due to lack of CRA Certification Schemes**

Application & Implementation Stages

SECURE online platform

SECURE
Cyber Resilience for SMEs

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 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. 2 Months
- **Applicants To Dos:** Sign & Submit Sub-GA

PUBLIC LINK TO SECURE ONLINE PLATFORM HAS BEEN SHARED ON THE WEBSITE ON 28th OF JANUARY

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

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Related Call Official Document = ***ANNEX 1 - Open Calls Application Guidelines***

SECURE
Cyber Resilience for SMEs

APPLICATION & IMPLEMENTATION PROCESS

SECURE
Cyber Resilience for SMEs

STAGE 1 – Registration & Proposal Submission

Phase 1 – Registration & Company Documentation upload

SECURE
Cyber Resilience for SMEs

Platform Activities

1. Register User on the online Platform
2. Fill in the Company registration data forms
3. Fill in the Bank account registration form
4. Fill in the self declaration form
5. **Download Sign & Upload Mandatory Documents**

Document Name	Where do I find it?	What should I do next?
1.Company Self Declaration	*Download it directly from the Online Platform (automatically generated by the platform)*	*Read it, digitally sign it and re-upload it on the platform*
2.ANNEX 3 - Ownership Control Declaration	*Download the template from the website*	*Fill it, digitally sign it and upload it on the platform*
3.Valid Registration Report + Company Good Standing Statement + shareholders + ownership graph	*Those documents are normally issued by National Chamber of Commerce or equivalent authorities. Refer to your relevant national authority to gather the necessary documentation.*	*If Registration report, shareholders and ownership graph are issued in a single document upload the same doc. in all the required field. Otherwise you can normally use the dedicated fields.*
4.Company Financial Statement (balance/turnover etc)	*This document is drafted directly from the company*	*Draft, sign and upload the document on the platform*
5.Other Documents if required	*If necessary NCCs can send uploading requests from the platform*	*Read the requests on notification section and upload the documents on the platform*

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Related Call Official Document = ***ANNEX 1 - Open Calls Application Guidelines; ANNEX 3-Ownership Control Declaration; ANNEX 4 - Valid Registration Report; ANNEX 4.1 - Company Financial Statement***

Phase 2 – Proposal & Budget Drafting

SECURE
Cyber Resilience for SMEs

Platform Activities

6. **Fill in Project Estimated Costs Fields**
7. **Ask for Prefinancing, if needed (box check)**
8. **Download, complete and sign the Project Proposal**
9. **Download, complete and sign the Proposal Budget**
10. **Submit the proposal**

Project Proposal (download on website)

- **Applicant Profile**
  - *Company description*
  - *Team & Suppliers*
- **Project Relevance**
  - *CRA goals*
  - *Objectives*
  - *Methodology*
- **Expected Impact**
  - *Outcomes for SMEs*
  - *KPIs*
- **WORK PACKAGES**
  - *Task, Milestones Deliverable & KPIs quantifications*

Proposal Budget (download on website)

Direct costs	Amount
Personnel costs	0,00 €
Subcontracting costs	0,00 €
Equipment costs	0,00 €
Purchase costs	0,00 €
Total direct costs	**0,00 €**
Indirect costs (7% of direct costs)	**0,00 €**
Total project budget	**0,00 €**
Max SECURE grant	

See Slide 21

Be sure to indicate misurable and realistic KPIs and clear activities. Consistency between costs and activities will be considered during the evaluation

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

*Related Call Official Document = **ANNEX 1 - Open Calls Application Guidelines; ANNEX 1.1-Proposal Template; ANNEX 1.2-Proposal Budget Guidelines; ANNEX 1.3-Proposal Budget Template***

Phase 3 - Proposal Evaluation

SECURE
Cyber Resilience for SMEs

Proposal Formal Evaluation
(Evaluation of CRA-Related Requirement)

Will be carried out by:
Cyber 4.0, SECURE Project Partner in charge for Financial Support Activities

Will assess:
- If the company falls under the CRA scope
- If the activities described in the proposal are eligible

Possible Outcomes:
- Proposal Approval
- Proposal Rejection

Outcomes will be communicated a week after the call closure

TECHNICAL EVALUATION

Will be carried out by:
An independent Evaluation Committee (members will be selected among SECURE Partners' personnel)

Will assess:
- The Score of the proposal-based specific evaluation parameters

Possible Outcomes:
- Financiable Proposal (RANKING)
- Not Financiable Proposal
  - *Under Treshold Score*
  - *Lowest Scores Exceeding Budget*

Outcomes will be communicated after the Company Eligibility Evaluation (duration: 2 months)

Company Eligibility Evaluation
(NCCs check on Company Documentation)

Will be carried out by:
NCCs, as an external endorsing actor of the SCURE Project.

Will assess:
- The truthfulness of Company Declarations
- The authenticity of the documentation
- Dimension and location of the Applicant

Possible Outcomes:
- Company Approval
- Company Rejection

Outcomes will be communicated a week after at least 2 months after the technical evaluation

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

*Related Call Official Document = **ANNEX 1 - Open Calls Application Guidelines***

Technical Evaluation Criteria (1/2)

Individual Evaluation Parameters

SECURE
Cyber Resilience for SMEs

Evaluation Committee will assess the proposal scores by **individual evaluation** and though **Consensus Meetings.**

There will be at least 3 evaluators for each single proposal

Individual evaluations will refer to the following parameters.

CRITERIA	Focus
Excellence and Relevance	1. *Relevance to EU cybersecurity goals on CRA* 2. *Project objectives and methodology* 3. *Resources and capabilities*
Impact and Clarity	1. *Expected outcomes for the SME* 2. *Clarity of Description* 3. *Indicators and KPIs to measure success*
Implementation	1. *Work Packages (WP)* 2. *Deliverables, Evidences and cost consistency* 3. *References to other EU Projects*

Score	Evaluation
0 = N/A	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.

Technical Evaluation Criteria (2/2)

Consensus Meeting Scoring and Ranking

SECURE
Cyber Resilience for SMEs

During Consensus Meetings the group of Evaluators who scored a single proposal will calculate the final score that will determine the ranking, following specific calculation rules:

1. The final score for each criterion will be the sum of the evaluators' scores, **with a maximum score of 15 points for each criterion**
2. The overall final score will be the weighted average of all criteria, with a **maximum total score of 15** considering the weights in the table

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	

Final Ranking

Proposals will be ranked all together, based on their final scores

Tresholds:

- **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.

Tie braking rules:

Proposals submitted earlier will be ranked higher than those submitted later. Amendment periods will not be considered.

Budget Limitations

In case of Call budget exhaustion lowest-ranked Proposals out of budget limit will be excluded

Phase 4 - Results & Sub Grant Signing

SECURE
Cyber Resilience for SMEs

Platform Activities

1. **EVALUATION RESULTS**
2. **If proposal has been admitted: download sign and re-upload Sub-Grant Agreement**
3. **Amend Material Errors if requested**
4. **Wait and download the coutersigned Sub-Grant Agreement**
5. **Receive the Prefinancing if requested**

Evaluation Phase	Exclusions Scenarios Summary	Aknowledgement by Applicant (Approximately)
Formal Evaluation (CRA-related requirements	1. The company does not, may not and will not fall under CRA scope **AND/OR** 2. The proposed project activities are not eligible **OR**	*After approximately 1 week after the Call closure*
Technical Evaluation	1. Final Proposal Score does not reach the minimum tresholds **OR** 2. The Proposal is out of budget limit as one of the lowest-ranked proposals (in case of budget exhaution) **OR**	*After the Company Eligibility Evaluation (duration approximately 2 months)*
Company Eligibility Evaluation	1. Company does not match one or more of the Company Eligibility Requirements **AND/OR** 2. Company's Member State NCC does not provide the evaluation	*After at least 2 months from the Technical Evaluation Closure*

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Phase 4 – Errors, Amendments and Sub-Grant Signing

SECURE
Cyber Resilience for SMEs

What shall I do if I identify an error after the Proposal Submission?

BEFORE THE CALL CLOSURE

Restart the application process with a different account, upload a new proposal and inform SECURE Staff:

submission-support@secure4sme.eu

AFTER THE CALL CLOSURE

You shall wait for SECURE Staff Communications

Formal Evaluation

If a manifest formal error is detected and it cannot be considered a Material Error your proposal will be rejected and you'll be informed by March 3, 2026

Technical Evaluation

In case of Material Errors of suspected Formal Errors the Evaluation Committee could contact you only to ask clarifications. *!!Clarifications provided will not affect the final score of your proposals; only Technical proposals contents will be evaluated!!*

Sub-Grant Signing

If after the provided clarifications the Evaluation Committee confirms a Material Error: you will be asked by Cyber 4.0 Staff to amend the error before signing the Sub-GA. In case of Formal Errors your Proposal may be considered invalid. You will be informed but you will not receive the Sub-GA

Formal Error

A formal error is an administrative or procedural error related to the form or completeness of the application. If such an error is identified in the submitted project proposal during the Formal Evaluation phase, the proposal will be rejected. Examples include missing mandatory documents, ineligible costs, failure to complete the required templates, missing or invalid signatures.

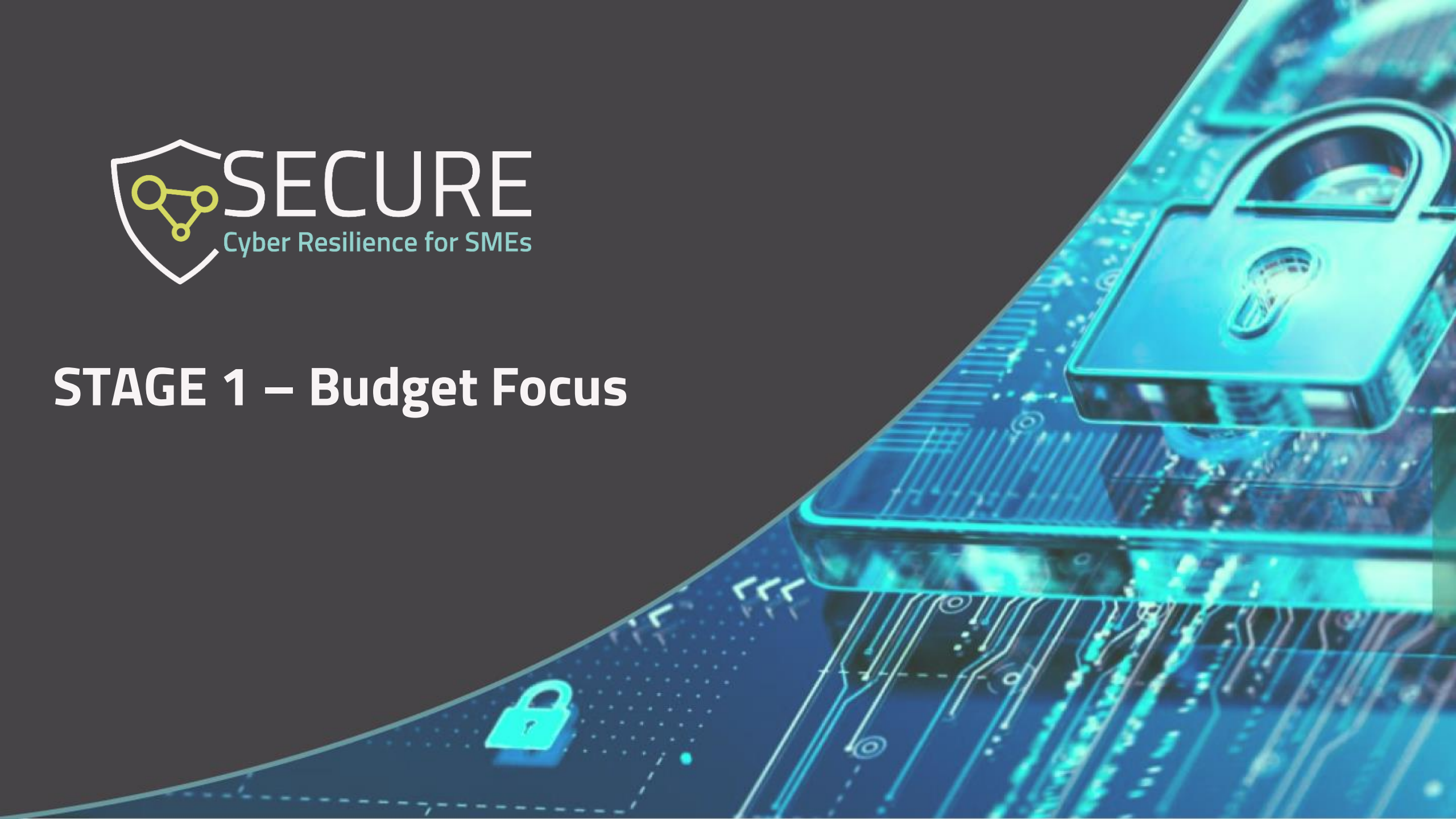
Material Error

A material error refers to minor inaccuracies or oversights in the proposal that do not affect the eligibility of the project. These may include typographical mistakes, formatting issues, or small inconsistencies in the documentation. Such errors may be subject to a clarification request by the Evaluation Committee during the Technical Evaluation and can be amended before the Sub-GA signing upon Cyber 4.0 request.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SECURE
Cyber Resilience for SMEs

STAGE 1 – Budget Focus



Reporting Methods & Eligible Costs

SECURE
Cyber Resilience for SMEs

Lump Sum Funding Mechanism

Not Needed

Actual Cost Reporting at any stage of the project

Needed

- Breakdown of estimated eligible costs by budget category
- Evidences for the achieved objectives

The Cost esteem will be used during the Proposal Evaluation to assess the consistency of the project activities with the expected costs

Eligible Costs *(can be co-financed)*

Direct Costs

- **Personnel Costs** - *Employees; natural persons direct contracts; seconded persons; SME owner and natural person beneficiary.*
- **Subcontracting costs** - *service providers, consultancy etc. – Must be registered in EU or EFTA MS; not controlled by countries outside EU/EFTA.*
- **Equipment** - *The total cost of equipment may not exceed 80% of total direct costs.*
- **Purchase cost** - *consumable and supplies, promotion, dissemination, results protection, publications, certificates etc.*

Indirect Costs

Flat rate of 7% of the total eligible costs (included in the max. financing of EUR 30,000)

Ineligible costs *(cannot be cofinanced)*

Return on capital, debt and debt service charges, provisions for losses or debts, interest owed, currency exchange losses, excessive or reckless expenditure, costs already funded by another EU action, alcoholic beverages, gifts or entertainment expenses, travel costs

Phase 2 - Eligible Costs - Direct costs

SECURE
Cyber Resilience for SMEs

Cost of **the time worked for the project** by:

- Employees
- Natural person under direct contract
- Seconded person
- SME owners and natural person beneficiaries

The **assignment to third parties, by contract, of specific tasks of the project action**, without transferring overall **responsibility for the action**, which **remains with** the cascading grant **beneficiary**

Instrumental assets, infrastructure, or other fixed assets necessary for project implementation. Eligible costs are calculated as **depreciation quota proportional to the project duration and the rate of actual use for project activities**

Costs for goods and services from external suppliers supporting project activities (e.g., consumables, dissemination, certificates, translations, publications)

Funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Phase 2 - Writing a SECURE lump sum proposal

SECURE
Cyber Resilience for SMEs

Prepare your application

- Use the proposal budget template & Proposal Template available on SECURE website
- Fill in the Proposal Template and Proposal Budget
- Describe in detail the activities covered by each work package

Justifying the budget

- All costs must be expressed in EUR (€)
- Estimations must approximate your actual costs
- Costs must comply with the eligibility criteria of the Digital Europe Programme Annotated Grant Agreement (DEP AGA), as explained in the Proposal Budget Guidelines
- Although the grant is a lump sum, the calculation must be based on realistic cost assumptions

Ensure consistency

Budget coherence and internal consistency

- **All cost items must be clearly linked to the activities described in the technical proposal.**
- **Assumptions must be understandable and costs necessary, avoiding over- or under-budgeting.**

Correct budget allocation

- All costs must be entered under the appropriate category.
- Avoid incorrect or "catch-all" allocations.

Suppliers shall be mentioned and described within the technical proposal

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Equipment costs focus

SECURE
Cyber Resilience for SMEs

Definition: Instrumental assets, infrastructure or other fixed assets necessary for the implementation of the project

Eligibility rules (DEP AGA):

- Only **depreciation costs** are eligible (not full purchase cost)
- Depreciation must be **proportional to the project duration** and actual use for project activities

Additional rule (First SECURE Open Call): Equipment costs cannot exceed **80% of total eligible costs**

Examples:

- Depreciation of a firewall used for cybersecurity testing activities
- Depreciation of a server purchased and used for project activities
- Depreciation of laptops assigned to personnel working on the project

Equipment vs Subcontracting examples:

- A **server purchased** by the beneficiary and used for project activities → **Equipment**
- A **server set as a specific procurement task** in the project and purchased through a third party → **Subcontracting**
- **Cybersecurity hardware purchased** by the beneficiary → **Equipment**
- **Cybersecurity hardware procurement set as a project task** carried out by a third party → **Subcontracting**

Please, ***provide a clear and detailed breakdown of equipment costs with a brief description for each item***, to enable evaluators to verify that each cost is correctly allocated to its budget category

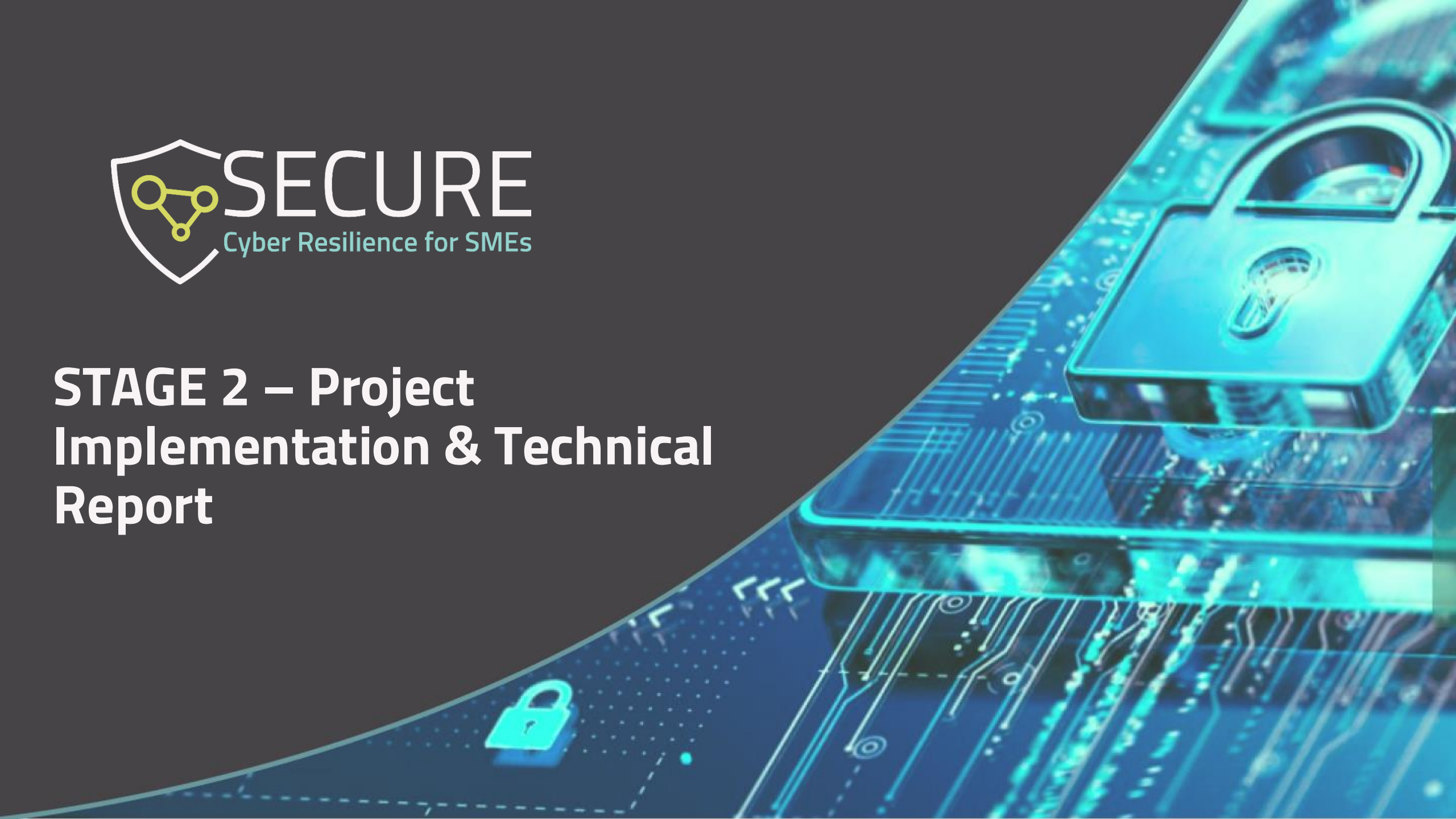
Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Reference: DEP AGA Article 6.2.C.2

SECURE
Cyber Resilience for SMEs

STAGE 2 – Project Implementation & Technical Report



Phase 5 – Initial CRA Maturity Assessment

SECURE
Cyber Resilience for SMEs

Platform Activities

1. **Download CRA Maturity Assessment Survey**
2. **Fill in the CRA Maturity Assessment Survey**
3. **Fill in the platform mandatory field with the results of the CRA Maturity Assessment Survey and upload the filled file on the platform**

Domain	Question	Answer	Domain score	Cyber Resilience Level
1. Asset Management & Classification	Do you maintain an up-to-date inventory of all IT assets (devices, systems, applications)?		#N/A	#N/A
	Are business-critical assets identified and classified by importance?			
	Do you document where sensitive data (e.g., customer, financial, HR) is stored?			
	Are asset owners formally assigned?			
	Are obsolete or unused assets decommissioned securely?			
2. Access Control & Authentication	Are unique accounts used for every employee (no shared accounts)?		#N/A	
	Is multi-factor authentication (MFA) enabled for critical systems and remote access?			
	Are privileged accounts (admin rights) restricted to those who need them?			
	Are access rights reviewed at least annually (or when staff leave/change roles)?			
	Are passwords required to follow a minimum standard (length, complexity)?			
	Are dormant or unused accounts disabled or removed promptly?			
3. Data Protection & Backup	Is sensitive data encrypted at rest (storage, devices) where appropriate?		#N/A	
	Is sensitive data encrypted in transit (emails, file transfers)?			
	Are regular backups performed for business-critical data?			
	Are backups stored offline or in a separate secure environment?			
	Are backups tested regularly to confirm they can be restored?			
4. Patch & Vulnerability Management	Are operating systems and applications kept up to date with the latest security patches?		#N/A	
	Is there a defined process for applying updates (automated or scheduled)?			
	Are unsupported systems or software replaced or isolated?			
	Are vulnerability scans conducted regularly on key systems?			
5. Awareness & Training	Have all employees received basic cybersecurity awareness training?		#N/A	
	Are phishing simulations or awareness tests conducted at least annually?			
	Do employees know how to report suspicious emails or cyber incidents?			
6. Incident Management & Monitoring	Is there an incident response plan that defines roles and responsibilities?		#N/A	
	Are security events (e.g., failed logins, malware alerts) monitored and logged?			
	Is there a defined process to escalate and respond to security incidents?			
	Are incidents documented and lessons learned integrated into improvements?			
7. Third-Party / Supplier Security	Are third-party IT providers assessed for minimum security practices?		#N/A	
	Are contracts with suppliers reviewed to ensure security responsibilities are defined?			
	Do you verify that external/cloud services protect data according to our requirements (e.g., backups, access control)?			

- Completion of the CRA Maturity Assessment is **MANDATORY**
- **Until the CRA Maturity Assessment has been uploaded to the platform, the Beneficiaries will not be allowed to upload the Technical Report**
- CRA Maturity Assessment will be available from Sub-Ga signing until upload of the Technical Report
- This does not prevent the Beneficiary from starting the Project implementation activities or from drafting the Technical Report offline

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Related Call Official Document = ***ANNEX 1 - Open Calls Application Guidelines***

Phase 6 – Implementation & Technical Report

SECURE
Cyber Resilience for SMEs

Platform Activities

1. **Download the Technical Report Template** → 1.1 IMPLEMENT THE PROJECT
2. **Complete the Technical Report**
3. **Sign and upload the Technical Report on the platform**
4. **Upload documents such as specific Deliverables and evidences, if necessary**

Technical Report (download on website)

- **Results**
  - *WPs, Tasks, Milestones, Deliverables*
- **Management, Impact and Ethics**
  - *Management, resources and costs justification*
  - *Impact*
  - *Ethical Issues, Security Issues, Data Protection and GDPR Compliance*
- **List of Annexes**

	Within these 180 days, beneficiaries must complete the full project implementation and submit the Technical Report.
	**Timing**: from the signing of Sub-Ga and for the duration of 180 days
	After the Technical Report is submitted, no further changes to the uploaded material will be allowed, unless specifically requested by the Evaluation Committee (see next slide)
	The Evaluation Committee will assess the deliverables only after the end of the 180-day period; early submission is allowed but does not lead to early payment.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Related Call Official Document = ***ANNEX 1 - Open Calls Application Guidelines*** and ***ANNEX 6 – Technical Report Template***

Phase 7 – Implementation Assessment, Payment & Attestation

SECURE
Cyber Resilience for SMEs

Platform Activities

1. **Implementation evaluation**
2. **If requested by Ev.Co., implement Technical Report amendments request**
3. **Complete Technical Report Amendments**
4. **Receive Balance payment**
5. **Complete Surveys and download the Attestation of project completion**

Evaluation Committee *will assess the Technical Reports comparing them with the Proposal and the uploaded evidence*

Possible Outputs of the Implementation Assessment

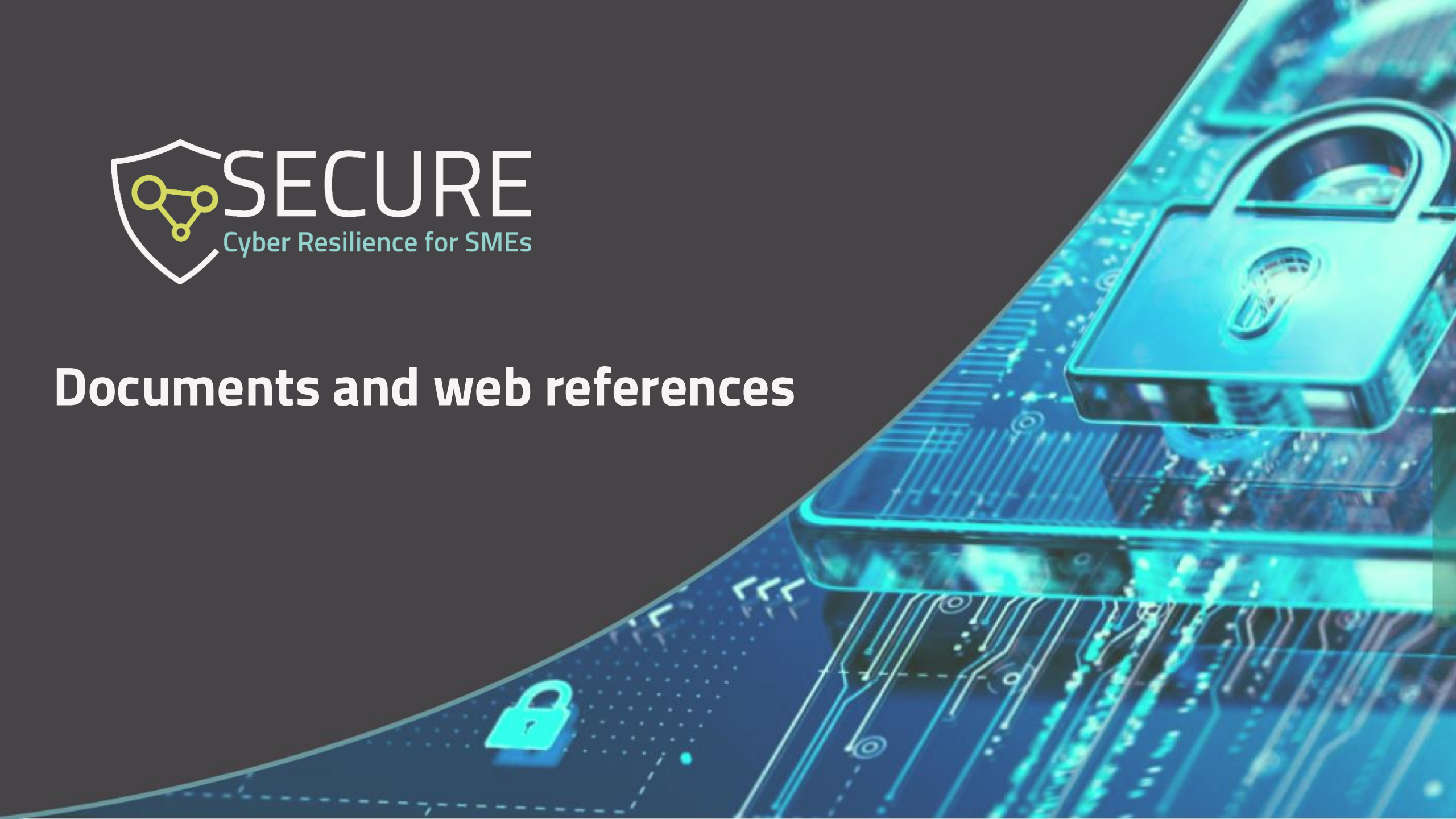
	Achieved	Partially Achieved	Not Achieved
Objectives and KPIs Achievement Assessment (Ev.Co)	The Evaluation Committee confirms that the project has been fully implemented and that all objectives and KPIs defined in the proposal have been achieved.	The Evaluation Committee determines that the project has been only partially implemented and identifies the level of achievement of the objectives and KPIs.	The Evaluation Committee concludes that the project has not been implemented and that the objectives and KPIs have not been achieved.
% of fundable Balance (Cyber 4.0)	**100%** The beneficiary receives the full balance corresponding to the total grant amount specified in the Sub-GA, minus any pre-financing already disbursed.	**TBD %** The balance payment is recalculated proportionally to the percentage of project completion. Any pre-financing already paid is deducted from the final balance. If the pre-financing exceeds the amount finally awarded, the beneficiary must reimburse the difference.	**0%** No balance payment is granted. Any pre-financing already received must be reimbursed
EXAMPLES **Grant amount = 30k €;** **Prefinancing = 12k €;**	*Applicant **receives** 18k € Balance*	*Achieved objectives 50%;* *Fundable balance = 15 k €;* *Applicant **receives**: 2 k €* *(balance – prefinancing)*	*Applicant shall **return** 12k €*

Related Call Official Document = ***ANNEX 1 - Open Calls Application Guidelines***

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SECURE
Cyber Resilience for SMEs

Documents and web references



Project Annexes List

ANNEX NAME	ANNEX DESCRIPTION
ANNEX 1 – Open Call Application Guidelines	Main Call Document containing all the basic information on Eligibility and Application & Implementation Process
ANNEX 1.1-Proposal Template	Download this document from the website, use it to draft your Project Proposal and upload a filled clean version on the platform
ANNEX 1.2-Proposal Budget Guidelines	Download this document from the website and use it as a guidance during the definition of the Proposal Budget (ANNEX 1.3 – Proposal Budget Template)
ANNEX 1.3-Proposal Budget Template	Download this document from the website, use it to estimate the Project Budget and upload a filled clean PDF version on the platform
ANNEX 2-CRA Scope & Eligible Activities, Services and Goods	Download this document from the website and use it as a guidance to understand CRA-related requirements and a list of eligible activities
ANNEX 3-Ownership Control Declaration	Download this document from the website with your company data and upload it on the platform
ANNEX 4 - Valid Registration Report with company good standing statement, shareholders and Ownership graphs	Request this document to yous National Chamber of Commerce or equivalent Authority and upload it on the required field in the platform
ANNEX 4.1 - Company Financial Statement	Produced annualy by each company (balance/turnover etc…)
Company Self-Declaration (platform annex)	Will be automatically generated by the platform with all the information provided by the Company: download it from the platform, read it, sign it and re-upload it
Sub- Grant Agreement (platform annex)	Will be automatically generated by the platform if the Proposal is admitted to financing: download it from the platform, read it, sign it and re-upload it

All Relevant Documents must be digitally signed in PadES format

Funded by the European Union

Contacts and Other Information

- **WEBSITE**: https://www.secure4sme.eu/about-secure
- **FAQ**: https://www.secure4sme.eu/faq
- **For questions on Open Calls please contact**: submission-support@secure4sme.eu
- **For other questions** (CRA Regulation, SECURE project, Other EU Projects, Dissemination, Events, etc.) **please contact**: info@secure4sme.eu
- **Online Contact Form:** https://www.secure4sme.eu/contacts
- **Newsletter**: https://www.secure4sme.eu/newsletter
- **News and Events:** https://www.secure4sme.eu/news-events
- **National (Cybersecurity) Coordination Centres**: https://cybersecurity-centre.europa.eu/nccs_en

Funded by the European Union

Thank you!

Website: www.secure4sme.eu

Contact Mail: info@secure4sme.eu

Linked In

Youtube

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 disclaimer: The project is supported by the European Cybersecurity Competence Center and its members.