SECURE

Cyber Resilience for SMEs

Dissemination Day Rome

25th February 2026

9.30 - 14.00 (CET)

Hybrid Event

Funded by the European Union

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

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

Institutional Session & Official Opening

Luca Nicoletti
Head of Industrial, Technological and Research Unit (ACN) and Head of the NCC-IT - ACN

Luca Tagliaretti
Executive Director, European Cybersecurity Competence Centre (ECCC)

Tjabbe Bos
Policy officer, Cybersecurity and Digital Privacy Policy, European Commission, DG CONNECT

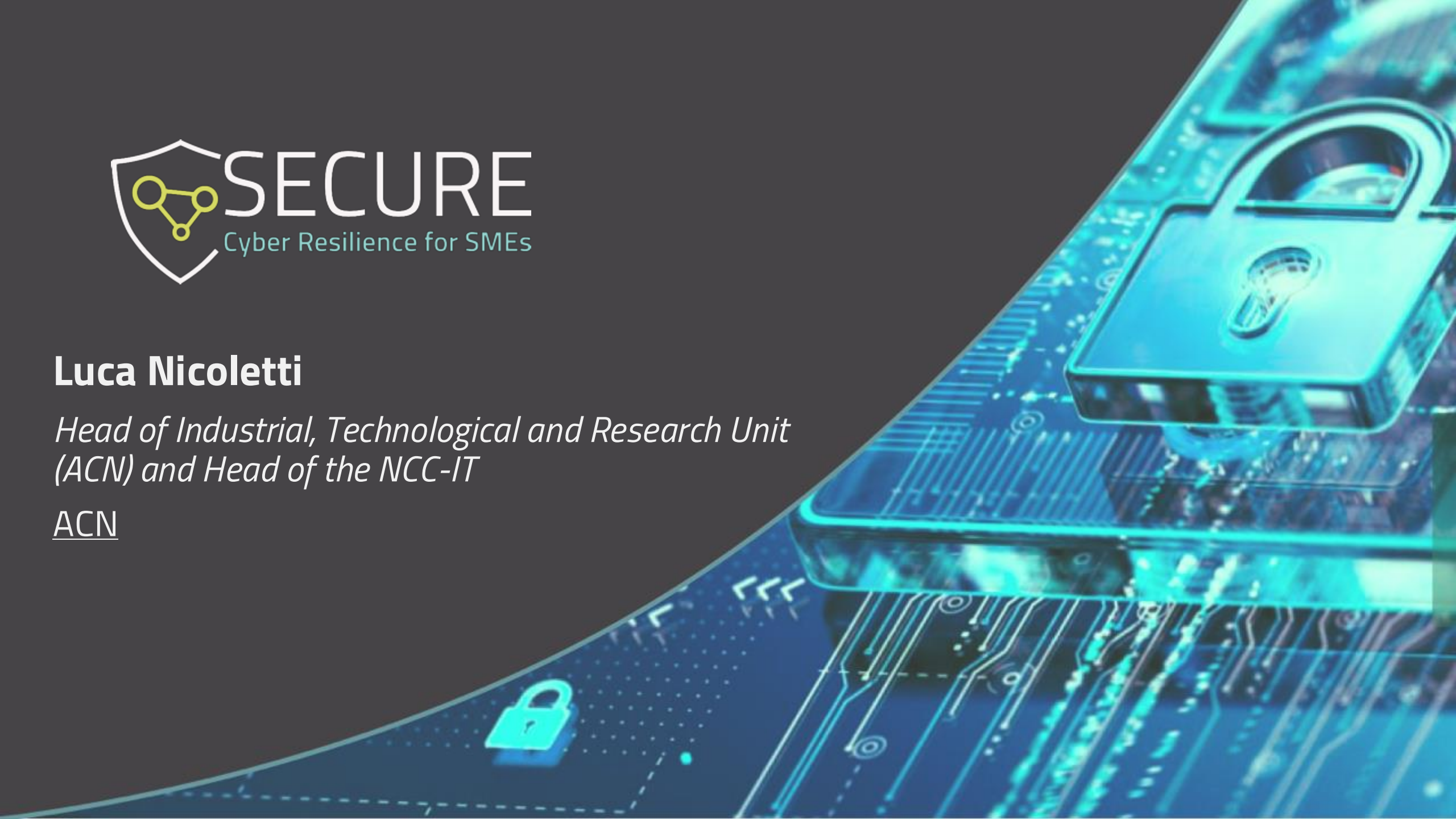
Paolo Spagnoletti
President, Cyber 4.0- Full Professor, Luiss University – Cyber 4.0 Competence Center

Funded by the European Union

ECCC

SECURE
Cyber Resilience for SMEs

SECURE
Cyber Resilience for SMEs



Luca Nicoletti

Head of Industrial, Technological and Research Unit (ACN) and Head of the NCC-IT

ACN

SECURE Project Overview

SECURE
Cyber Resilience for SMEs

General Objective of the SECURE project

Support European **SMEs**, with a focus on micro and small enterprises, to **strengthen their cybersecurity capacities and to support the implementation of the proposed Regulation on CRA**

General information

Total Budget: 22 mln €	Funded by DIGITAL-DEPLOY-CYBER-06-STRENGTHENCRA	**Length: 3 years**
FSTP's Budget: 16.5 mln €		**Start Date: 1 January 2025**

Main Objective's

- **Managing Open Calls** by ensuring impartial evaluation and transparent monitoring of cascade funding
- Ensuring European SMEs' **awareness, accessibility and engagement** for cascade financing
- Establishing **CRA compliance resources;** online **platform** as main vehicle for upskilling and capacity building
- Performing **trainings and upskilling** of stakeholders to achieve CRA compliance
- Promoting knowledge sharing and facilitating **CRA Compliance Use Cases**
- Contributing to **CRA Standardisation** efforts by engaging with European and International Bodies

8 Partners

5 NCCs
3 organisations

Consortium

ACN · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · NCC-BE · NCC CENTRUL NAȚIONAL DE COORDONARE CYBERSECURITY ROMÂNIA · LHC Luxembourg House of Cybersecurity · CYBER 4.0 · NASK · INDUSTRIE 4.0 ÖSTERREICH

Affiliated Entities

ideare ideas & research hub

External Contributors

ECCC

NCCs or relevant national authorities of all EU27 and EEA/EFTA countries

Open calls for European SMEs

SECURE Cyber Resilience for SMEs

SECURE provides for **financial support to third parties** (FSTPs) through open calls dedicated to **Micro, Small and Medium enterprises** across the European Union.

A series of open calls (2 or 3) will be published to co-finance Projects aimed at improving CRA compliance strengthening cybersecurity practices, and promoting a harmonised approach to resilience throughout the EU.

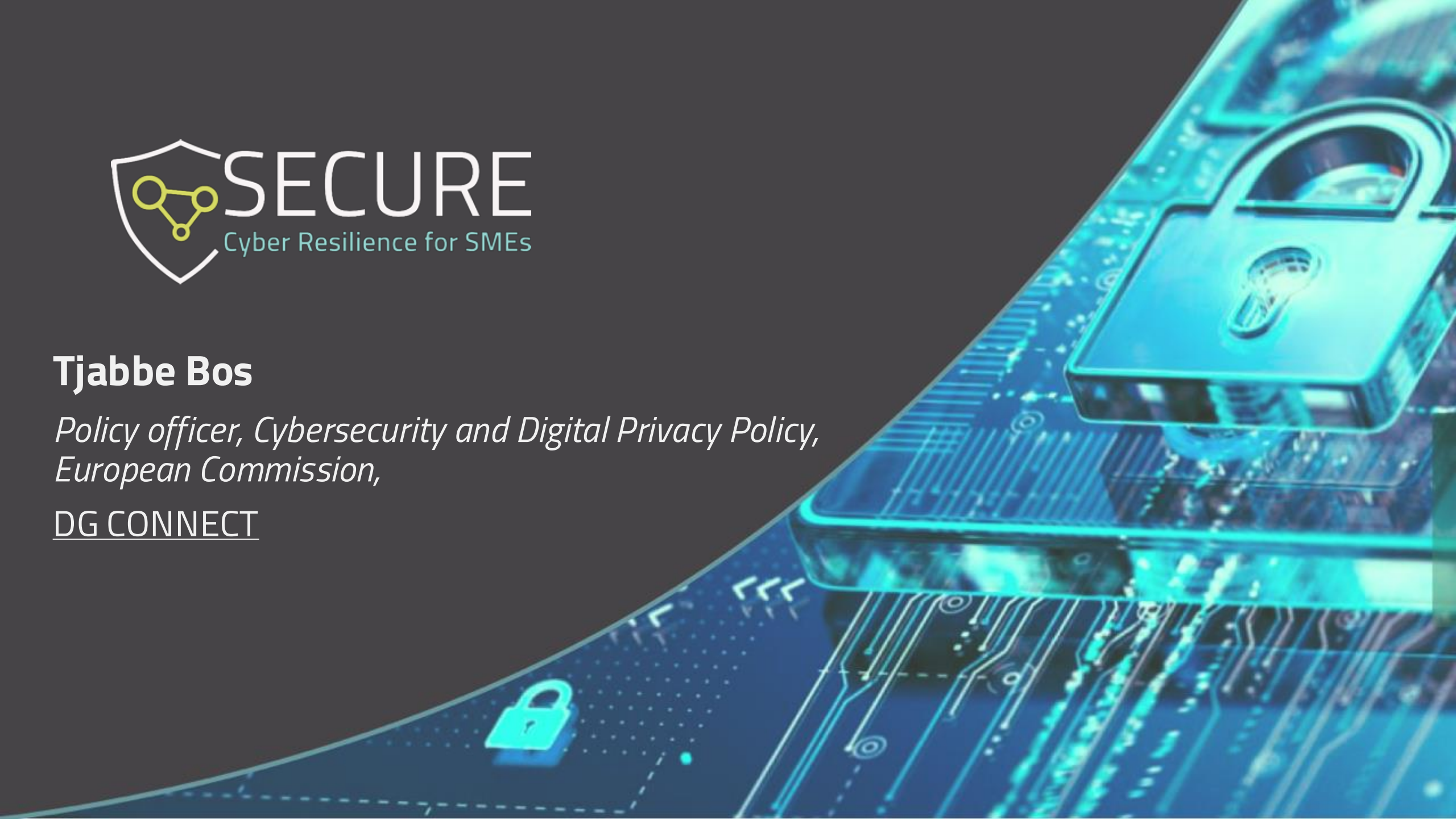
The first call has been launched end of **January 2026**. SMEs will have around 2 months to apply and to take the chance to be awarded up to €30.000 (50% of overall project costs) for realizing 6 months projects.

All updates and detailed guidelines soon available at the SECURE Website

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SECURE
Cyber Resilience for SMEs



Tjabbe Bos

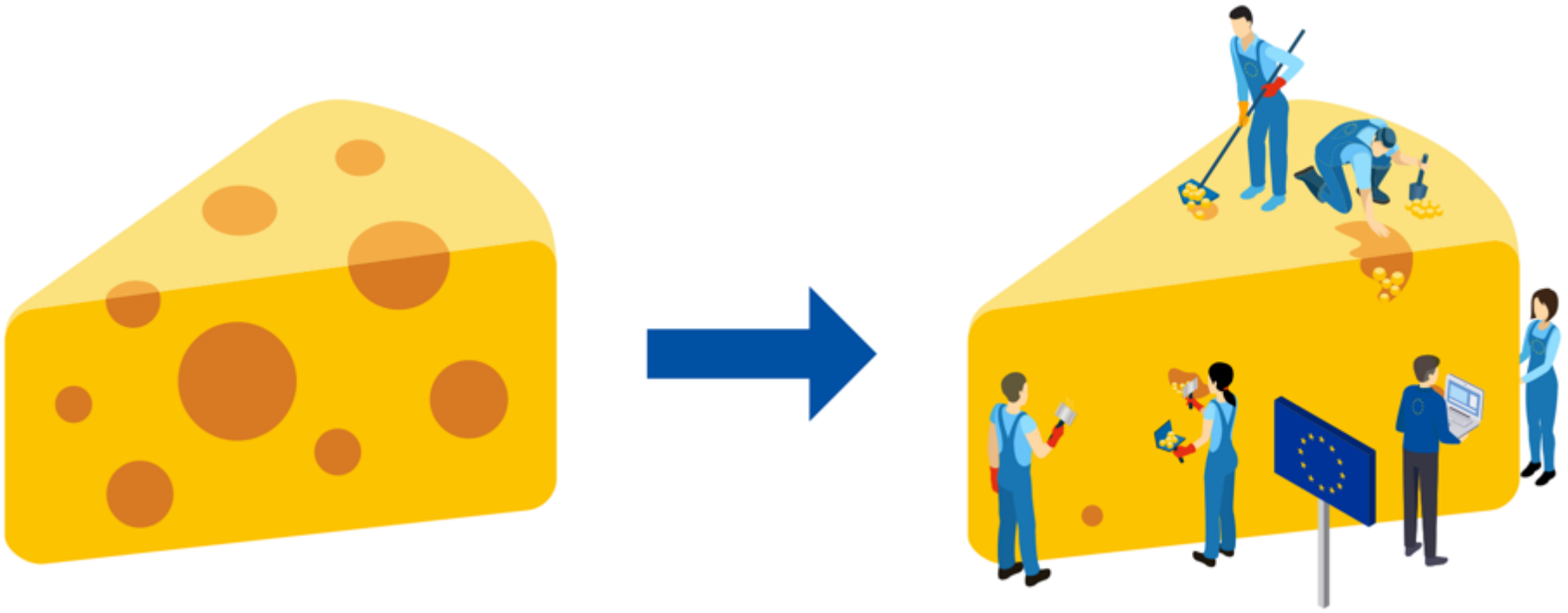
Policy officer, Cybersecurity and Digital Privacy Policy,
European Commission,

DG CONNECT

Cyber Resilience Act

European Commission, DG CONNECT

CRA in a nutshell



European Commission

State of play

Adoption of the Cyber Resilience Act (October 2024)

Impact - full application: December 2027

- Regulation = direct effect; no transposition via national laws
- Full harmonisation = 27 Member States cannot deviate for the scope covered

Implementation

- The European Commission is the guardian of the treaties and monitoring implementation of EU law & negotiates international trade agreements
- Multi-stakeholder process : Member States supervise and enforce/market surveillance; European harmonised standards developed with industry, etc.

Main elements of the CRA

- **Cybersecurity rules** for the placing on the market of hardware and software
- **Obligations** for manufacturers, importers and distributors
- Cybersecurity **essential requirements** across the life cycle
- Harmonised **standards** to support implementation
- **Conformity assessment** – differentiated by product category
- **Reporting** obligations – actively exploited vulnerabilities & severe incidents
- **Market surveillance and enforcement**

CRA implementation

- Adoption of lower level regulations
- Development of harmonised standards
- Guidance to support implementation
- Single Reporting Platform by ENISA
- Member States to set up notifying bodies (conformity assessment bodies) & market surveillance authorities

CRA implementation underway - MSMEs

- MSME support actions in CRA
  - Member State actions (awareness raising, training, communication channels, support testing and conformity assessment activities, regulatory sandboxes),
  - Commission actions (implementation guidance, advertise financial support, simplified technical documentation).
- Digital Europe Programme - SME support actions

SECURE
Cyber Resilience for SMEs

Luca Tagliaretti

Executive Director,

European Cybersecurity Competence Centre (ECCC)

SECURE
Cyber Resilience for SMEs

Paolo Spagnoletti

President, Cyber 4.0- Full Professor, Luiss University,

Cyber 4.0 Competence Center

SECURE

Cyber Resilience for SMEs

Dissemination Day Rome

25th February 2026

9.30 - 14.00 (CET)

Hybrid Event

Funded by the European Union

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

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

Roundtable

Manufacturing mSMEs Between Cyber Threats and Regulatory Compliance - Benefits and Impacts of the CRA

Matteo Macina
Member of the Cybersecurity Working Group – Assolombarda

Paolo Brizzi
Digital Factory Program Lead | CIO - CIM Competence Center

Stefanie Werderits
Project Manager & Policy Advisor - PIA (Plattform Industrie 4.0)

Lorenzo Patera
IT Program Manager - BI-REX Competence Center

Beatriz Garcia Del Pozo
Head of Regulation and Information Security Management - INCIBE

SECURE
Cyber Resilience for SMEs

Funded by the European Union

ECCC

Funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

SECURE
Cyber Resilience for SMEs

SECURE
Cyber Resilience for SMEs

Dissemination Day Rome

25th February 2026

9.30 - 14.00 (CET)

Hybrid Event

Funded by the European Union

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

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

The SECURE PROJECT

INTRODUCTION

Andrea Margheri
Division for Industrial and Technology Projects, Head of Division – ACN

CRA GUIDELINES

Yves Streel
Senior Program/Project Manager – CCB (NCC Belgium)

Szymon Barszczewski
Cybersecurity Certification Specialist – NASK

USE CASES

Carmelo Dimauro
Project Lead – NC3/LHC (NCC Luxembourg)

1st OPEN CALL

Alessandro Calabrese
Head of Advisory and Training - Cyber 4.0 Competence Center

SECURE
Cyber Resilience for SMEs

Funded by the European Union
ECCC

SECURE
Cyber Resilience for SMEs

Introducing the SECURE Project

Andrea Margheri

Division for Industrial and Technology Projects, Head of Division

ACN

SECURE Project Overview

SECURE
Cyber Resilience for SMEs

General Objective of the SECURE project		
Support European **SMEs**, with a focus on micro and small enterprises, to **strengthen their cybersecurity capacities and to support the implementation of the proposed Regulation on CRA**		
General information		
Total Budget: 22 mln €	Funded by DIGITAL-DEPLOY-CYBER-06-STRENGTHENCRA	**Length: 3 years**
FSTP's Budget: 16.5 mln €		**Start Date: 1 January 2025**

Main Objective's

- **Managing Open Calls** by ensuring impartial evaluation and transparent monitoring of cascade funding
- Ensuring European SMEs' **awareness, accessibility and engagement** for cascade financing
- Establishing **CRA compliance resources;** online **platform** as main vehicle for upskilling and capacity building
- Performing **trainings and upskilling** of stakeholders to achieve CRA compliance
- Promoting knowledge sharing and facilitating **CRA Compliance Use Cases**
- Contributing to **CRA Standardisation** efforts by engaging with European and International Bodies

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SECURE Project Consortium

SECURE
Cyber Resilience for SMEs

8 PARTNERS

5 NCCs & 3 ORGANISATIONS

The Consortium is represented by **7 EU countries:**

AFFILIATED ENTITIES

ideare
ideas & research hub

EXTERNAL CONTRIBUTORS

NCCs or relevant national authorities of all EU27 and EEA/EFTA countries

Funded by the European Union

Key information about cybersecurity of EU SMEs

SECURE
Cyber Resilience for SMEs

The SECURE project addresses one of the main cybersecurity challenges in Europe: **cybersecurity maturity**

99.8% of European businesses are SMEs.

>80% of SMEs process critical information (business, personal and sensitive)

62.65 out of 100 EU Cyber-Index in 2024 (ENISA)

~23 million EU SMEs accounting for 99% of businesses and two out of every three private sector jobs

21.5% of EU enterprises had ICT security incidents2023

52 out of 100, cybersecurity maturity of **Italian** SMEs (Cyber Index 2024)

Funded by the European

Sources: European Commission, Eurostat, ENISA, Cyber Index PMI

SECURE Project Structure

SECURE
Cyber Resilience for SMEs

WP1 - Initial stock taking and stakeholder engagement
Support to the identification of SMEs beneficiaries and NCCs'/other stakeholders' involvement into the project

Project Platform

WP2 - Access to finance and open calls for European SMEs
Establishment, and management of open calls applications and funds

WP3 - Creation and animation of the central repository
Creation and delivery of a multilingual platform acting as a repository for knowledge-sharing

Content development

WP4 - SMEs capacity enhancement
Development of training sessions, workshops, e-learning materials & toolkits for the platform, as well as industry-specific events

WP5 - National Use Cases
Organisation of information sharing among Member States (e.g. best practices, use cases, field experiences)

WP6 - Impact Creation: Development and implementation of a communication and dissemination strategy

WP7- Project Management and Coordination: Overall management of the project to ensure the correct on-going of its activities

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

NOW OPEN: First Open call for European SMEs

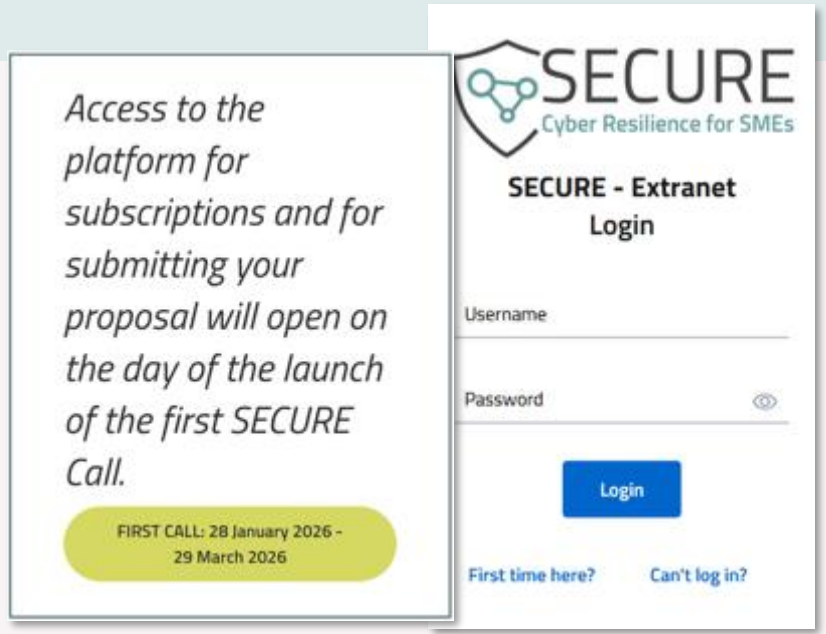
SECURE provides for **financial support to third parties** (FSTPs) through open calls dedicated to **Micro, Small and Medium enterprises** across the European Union.

The first call launched **January 28th 2026 and will close on March 29th 2026**. SMEs will have the chance to be awarded up to €30.000 (50% of overall project costs) for realizing 6 months projects.

A series of open calls (2 or 3) will be published to co-finance Projects aimed at improving CRA compliance strengthening cybersecurity practices, and promoting a harmonised approach to resilience throughout the EU.

SECURE Website

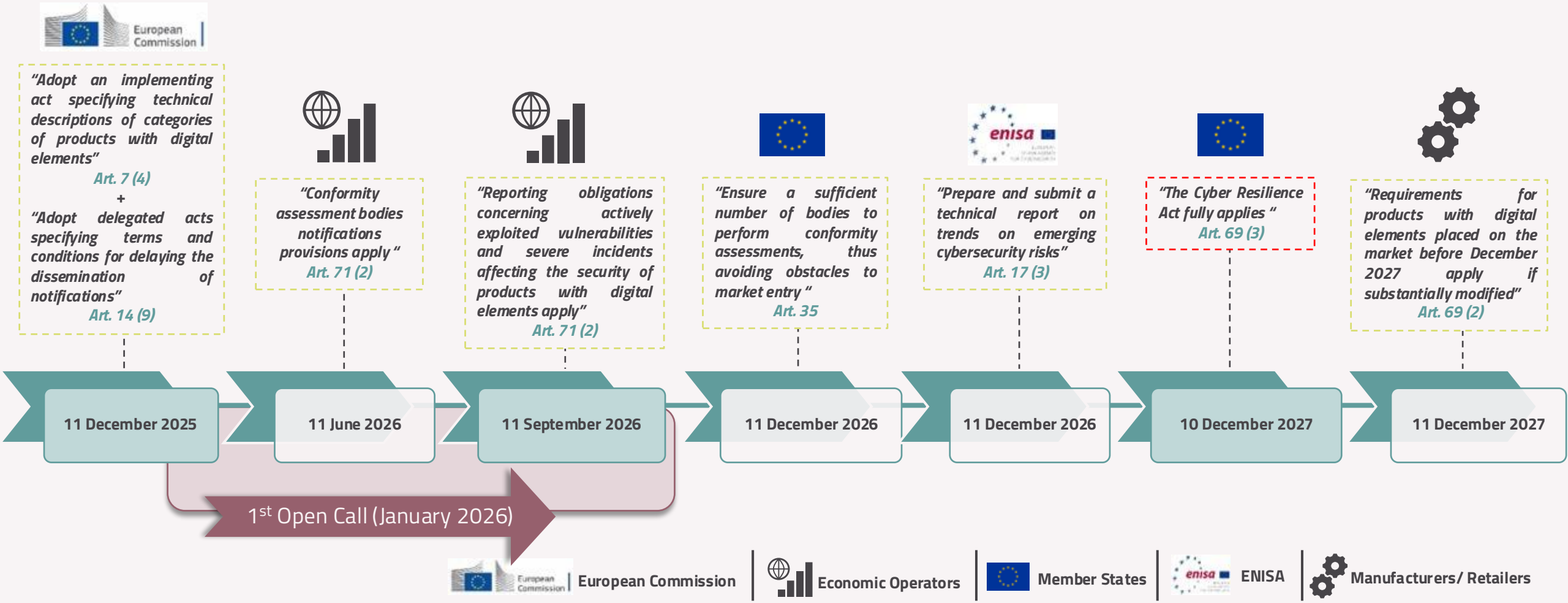
- Open Call application portal
- Updates of the SECURE Project
- Detailed guidelines
- CRA Maturity Score



Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Timeline of CRA implementation vs. First Open Call Schedule

SECURE
Cyber Resilience for SMEs



Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SECURE
Cyber Resilience for SMEs

CRA Guidelines

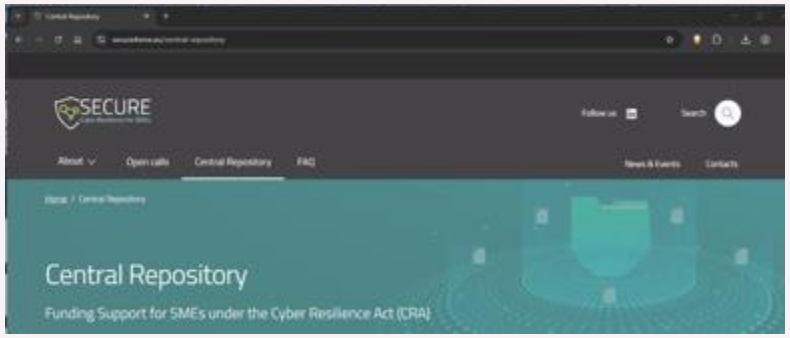
Yves Streel

Senior Program/Project Manager

CCB (NCC Belgium)

SECURE the knowledge: SME's capacity enhancement

Ensuring accessibility of CRA obligations



https://www.secure4sme.eu/central-repository

CRA evaluation tool

Question	Answer	Domain score	Cyber Resilience Level
Do you maintain an up-to-date inventory of all IT assets (devices, systems, applications)?	Partially	0,8	0,938095238
Are business-critical assets identified and classified by importance?	Partially		
Do you document where sensitive data (e.g., customer, financial, HR) is stored?	Partially		
Are asset owners formally assigned?	Partially		
Are obsolete or unused assets decommissioned securely?	No		
Are unique accounts used for every employee (no shared accounts)?	Partially	1,333333333	
Is multi-factor authentication (MFA) enabled for critical systems and remote access?	Partially		
Are privileged accounts (admin rights) restricted to those who need them?	Partially		
Are access rights reviewed at least annually (or when staff leave/change roles)?	Partially		
Are passwords required to follow a minimum standard (length, complexity)?	Yes		
Are dormant or unused accounts disabled or removed promptly?	Yes		
Is sensitive data encrypted at rest (storage, devices) where appropriate?	Yes	1,6	
Is sensitive data encrypted in transit (emails, file transfers)?	Yes		
Are regular backups performed for business-critical data?	Partially		
Are backups stored offline or in a separate secure environment?	Yes		
Are backups tested regularly to confirm they can be restored?	Partially		
Are operating systems and applications kept up to date with the latest security patches?	Partially	0,25	
Is there a defined process for applying updates (automated or scheduled)?	No		
Are unsupported systems or software replaced or isolated?	No		
Are vulnerability scans conducted regularly on key systems?	No		
Have all employees received basic cybersecurity awareness training?	No	0,666666667	
Are phishing simulations or awareness tests conducted at least annually?	No		
Do employees know how to report suspicious emails or cyber incidents?	Yes		
Is there an incident response plan that defines roles and responsibilities?	Partially	1,25	
Are security events (e.g., failed logins, malware alerts) monitored and logged?	Partially		
Is there a defined process to escalate and respond to security incidents?	Yes		
Are incidents documented and lessons learned integrated into improvements?	Partially		
Are third-party IT providers assessed for minimum security practices?	Partially	0,666666667	
Are contracts with suppliers reviewed to ensure security responsibilities are defined?	Partially		
Do you verify that external/cloud services protect data according to our requirements (e.g., backups, access contr	No		

Domain	Question	Answer	Domain Score	Product Resilience Level
1. Asset & Product Identification	Do you maintain a current inventory of all digital products under CRA scope?	Partially	1	0,738095238
	Are all digital products classified by criticality or exposure to cyber risks?	Partially		
	Are product versions and updates tracked systematically?	Yes		
	Do you identify which product components are vulnerable to cybersecurity threats?	Partially		
	Are responsibilities for each product clearly assigned?	No		
2. Security by Design & Development	Are security requirements integrated into the product design process?	Yes	1,166667	
	Do you conduct threat modeling for all CRA-relevant products?	Partially		
	Are security controls validated during product development?	Yes		
	Do you perform regular security testing (penetration, code review, fuzzing) before release?	Partially		
	Are secure coding guidelines applied across all development teams?	Partially		
	Are data privacy and protection measures (e.g., encryption) embedded into products by default?	No		
3. Vulnerability Management	Do you have a formal process for identifying vulnerabilities in our products (e.g., CVD)	Yes	1,4	
	Are vulnerabilities documented and tracked in a central repository?	Partially		
	Is there a defined timeline for applying security patches or updates?	Partially		
	Are vulnerability fixes tested before delivering to customers?	Yes		
	Do you maintain records of past vulnerabilities and how they were addressed?	Partially		
4. Supply Chain & Third-Party Components	Are all third-party components assessed for security before use?	Yes	0,5	
	Do you require suppliers to meet minimum cybersecurity standards?	No		
	Are supply chain risks reviewed regularly?	No		
	Do contracts with suppliers include clauses about vulnerability reporting and handling?	No		
5. Monitoring & Incident Response	Are security incidents detected and logged for all CRA-relevant products?	No	0,6	
	Is there a documented incident response plan aligned with CRA reporting obligations?	Partially		
	Are incident response roles and responsibilities clearly defined?	Partially		
	Are employees trained to recognize and report incidents promptly?	No		
	Do you regularly review and update incident response procedures?	Partially		
6. Compliance & Documentation	Are all security measures and risk assessments documented and maintained?	No	0	
	Can you provide evidence of due diligence and compliance with CRA if requested?	No		
	Are vulnerability handling reports ready for submission to competent authorities within CRA timelin	No		
7. Governance & Awarenes	Do all relevant teams (R&D, IT, legal, management) understand CRA obligations?	Partially	0,5	
	Are roles and responsibilities for CRA compliance formally assigned and communicated?	No		

*Hands-on **practical recommendations***

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CRA 101 understanding CRA obligations (1/4)

What SMEs Need to Know

- Cyber Resilience Act (EU) 2024/2847
- Applies to Products with Digital Elements (PDEs)
- Timeline: 2024 entry | 2026 reporting | 2027 full application
- Covers entire product lifecycle

Funded by the European Union

CRA 101 understanding CRA obligations (2/4)

1 Secure by Design – Risk Assessment

- Identify cybersecurity risks
- Document & update throughout support period
- Cover intended use & environment
- Include third-party components (SBOM)

2 Manage Vulnerabilities & Updates

- Identify & document vulnerabilities (SBOM)
- Provide free security updates without undue delay
- Maintain updates ≥10 years or support period
- Define minimum 5-year support period

Funded by the European Union

CRA 101 understanding CRA obligations (3/4)

3 Inform Users & 4 Report Incidents

- Provide secure-use instructions & product details
- Appoint Single Point of Contact (SPOC)
- 24h early warning | 72h notification
- Report to CSIRT, ENISA platform & users

5 Conformity & Technical Documentation

- EU Declaration of Conformity (EU DoC)
- CE Marking
- Appropriate conformity procedure
- Maintain complete technical documentation

Funded by the European Union

CRA 101 understanding CRA obligations (4/4)

- Beginner-friendly/basic level

CRA requires five core actions:

- Design securely (Risk Assessment)
- Manage vulnerabilities (Updates & SBOM)
- Inform users (Transparency & SPOC)
- Report incidents (24h/72h deadlines)
- Prove compliance (CE + Technical File)

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CRA essential cybersecurity requirements (1/4)

SECURE
Cyber Resilience for SMEs

4 pillars form the structural foundation of CRA compliance

Risk-Based Approach

Secure by Design & Default

Lifecycle Security

Supply Chain Security

Funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CRA essential cybersecurity requirements (2/4)

1 Risk-Based Cybersecurity Approach

- Ensure appropriate cybersecurity level based on risks
- Lifecycle risk assessment (Design → EOL)
- Identify assets, threats, vulnerabilities
- Impact × Likelihood prioritisation
- Traceability: risk → controls → evidence

2 Secure by Design & Development

- Security embedded from concept phase
- Secure defaults (no shared passwords, minimal exposure)
- Signed firmware & secure boot
- Secure coding (SAST, DAST, fuzzing)
- Systematic threat modelling

Funded by the European Union

CRA essential cybersecurity requirements (3/4)

3 Lifecycle Security Management

- Continuous vulnerability monitoring (CVE, SBOM)
- Timely signed updates with rollback
- Updates available ≥10 years or support period
- Public CVD policy & reporting channel
- Transparent communication

4 Supply Chain Security

- Maintain and update SBOM
- Monitor open-source & third-party risks
- Cybersecurity clauses in supplier contracts
- 24h reporting of critical supplier vulnerabilities
- CI/CD security gates for dependencies

Funded by the European Union

CRA essential cybersecurity requirements (4/4)

- Technical guideline on essential cybersecurity requirements (Annex I, Part I: point 1 and 2)
- Recognised best practices & existing standards
- **Four chapters**:
  1) Risk-based cybersecurity approach
     - Risk assessment
     - Tailored security measures
     - Reflection on threat models, attack surfaces & impacts
  2) Secure-by-design/default principle
  3) Security management duties (lifecycle)
  4) Supply chain considerations & controls

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CRA Maturity Score:
Organization cyber resilience level

SECURE
Cyber Resilience for SMEs

Question	Answer	Domain score	Cyber Resilience Level
Do you maintain an up-to-date inventory of all IT assets (devices, systems, applications)?	Partially	0,8	0,938095238
Are business-critical assets identified and classified by importance?	Partially		
Do you document where sensitive data (e.g., customer, financial, HR) is stored?	Partially		
Are asset owners formally assigned?	Partially		
Are obsolete or unused assets decommissioned securely?	No		
Are unique accounts used for every employee (no shared accounts)?	Partially	1,333333333	
Is multi-factor authentication (MFA) enabled for critical systems and remote access?	Partially		
Are privileged accounts (admin rights) restricted to those who need them?	Partially		
Are access rights reviewed at least annually (or when staff leave/change roles)?	Partially		
Are passwords required to follow a minimum standard (length, complexity)?	Yes		
Are dormant or unused accounts disabled or removed promptly?	Yes		
Is sensitive data encrypted at rest (storage, devices) where appropriate?	Yes	1,6	
Is sensitive data encrypted in transit (emails, file transfers)?	Yes		
Are regular backups performed for business-critical data?	Partially		
Are backups stored offline or in a separate secure environment?	Yes		
Are backups tested regularly to confirm they can be restored?	Partially		
Are operating systems and applications kept up to date with the latest security patches?	Partially	0,25	
Is there a defined process for applying updates (automated or scheduled)?	No		
Are unsupported systems or software replaced or isolated?	No		
Are vulnerability scans conducted regularly on key systems?	No		
Have all employees received basic cybersecurity awareness training?	No	0,666666667	
Are phishing simulations or awareness tests conducted at least annually?	No		
Do employees know how to report suspicious emails or cyber incidents?	Yes		
Is there an incident response plan that defines roles and responsibilities?	Partially	1,25	
Are security events (e.g., failed logins, malware alerts) monitored and logged?	Partially		
Is there a defined process to escalate and respond to security incidents?	Yes		
Are incidents documented and lessons learned integrated into improvements?	Partially		
Are third-party IT providers assessed for minimum security practices?	Partially	0,666666667	
Are contracts with suppliers reviewed to ensure security responsibilities are defined?	Partially		
Do you verify that external/cloud services protect data according to our requirements (e.g., backups, access contr	No		

0-1,25	Low
1,25-1,75	Medium
1,75-2	High

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CRA Maturity Score:
Product resilience level

SECURE
Cyber Resilience for SMEs

Domain	Question	Answer	Domain Score	Product Resilience Level
1. Asset & Product Identification	Do you maintain a current inventory of all digital products under CRA scope?	Partially	1	0,73809524
	Are all digital products classified by criticality or exposure to cyber risks?	Partially		
	Are product versions and updates tracked systematically?	Yes		
	Do you identify which product components are vulnerable to cybersecurity threats?	Partially		
	Are responsibilities for each product clearly assigned?	No		
2. Security by Design & Development	Are security requirements integrated into the product design process?	Yes	1,166667	
	Do you conduct threat modeling for all CRA-relevant products?	Partially		
	Are security controls validated during product development?	Yes		
	Do you perform regular security testing (penetration, code review, fuzzing) before release?	Partially		
	Are secure coding guidelines applied across all development teams?	Partially		
	Are data privacy and protection measures (e.g., encryption) embedded into products by default?	No		
3. Vulnerability Management	Do you have a formal process for identifying vulnerabilities in our products (e.g., CVD)	Yes	1,4	
	Are vulnerabilities documented and tracked in a central repository?	Partially		
	Is there a defined timeline for applying security patches or updates?	Partially		
	Are vulnerability fixes tested before delivering to customers?	Yes		
	Do you maintain records of past vulnerabilities and how they were addressed?	Partially		
4. Supply Chain & Third-Party Components	Are all third-party components assessed for security before use?	Yes	0,5	
	Do you require suppliers to meet minimum cybersecurity standards?	No		
	Are supply chain risks reviewed regularly?	No		
	Do contracts with suppliers include clauses about vulnerability reporting and handling?	No		
5. Monitoring & Incident Response	Are security incidents detected and logged for all CRA-relevant products?	No	0,6	
	Is there a documented incident response plan aligned with CRA reporting obligations?	Partially		
	Are incident response roles and responsibilities clearly defined?	Partially		
	Are employees trained to recognize and report incidents promptly?	No		
	Do you regularly review and update incident response procedures?	Partially		
6. Compliance & Documentation	Are all security measures and risk assessments documented and maintained?	No	0	
	Can you provide evidence of due diligence and compliance with CRA if requested?	No		
	Are vulnerability handling reports ready for submission to competent authorities within CRA timelin	No		
7. Governance & Awarenes	Do all relevant teams (R&D, IT, legal, management) understand CRA obligations?	Partially	0,5	
	Are roles and responsibilities for CRA compliance formally assigned and communicated?	No		

0-1,25	Low
1,25-1,75	Medium
1,75-2	High

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CRA Methodological Compliance Assessment Framework

- For SMEs to **evaluate & refine** their **CRA compliance**
- Suggests existing tools, standards, templates, checklists
- **Five criteria**:
    1) Essential cybersecurity requirements compliance
    2) Certification of products with digital elements
    3) Classification of products as Class I or II and corresponding actions
    4) Technical documentation completeness
    5) Overall conformity assessment procedures

SECURE CRA guidance – visual comparison

SECURE
Cyber Resilience for SMEs

CRA101 Understanding CRA Obligations

Level: **Legal Overview**

Focus:
- Key CRA obligations
- Risk assessment
- Reporting timelines
- EU DoC & CE marking

Role:
Awareness

Annex I, Part I Essential Cybersecurity Requirements

Level: **Technical Implementation**

Focus:
- Risk-based approach
- Secure-by-design/default
- Lifecycle security
- Supply chain security

Role:
Engineering

Methodological Compliance Assessment Framework

Level: **Governance & Compliance**

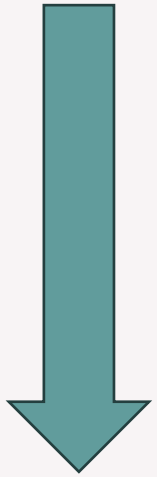
Focus:
- 21 Annex I requirements
- Classification pathways
- Conformity modules
- Technical documentation

Role:
Demonstration

Awareness → Implementation → Demonstration

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Conclusions



- CRA 101 : Understanding CRA Obligations
- CRA Essential Cybersecurity Requirements
- CRA Maturity Score
- CRA Methodological Compliance Assessment Framework

Funded by the European Union

SECURE
Cyber Resilience for SMEs

CRA Guidelines

Szymon Barszczewski

Cybersecurity Certification Specialist

NASK

Possible courses of action

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

NASK

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.

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

Products with digital elements (default category)

- Conformity assessment procedure based on internal control (based on module A)
- EU-type examination procedure (based on module B) followed by conformity to EU-type based on internal production control (based on module C)
- Conformity assessment based on full quality assurance (based on module H)
- (where available) European cybersecurity certification schemes

Funded by the European Union

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.

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

Important products with digital elements – Class I

SECURE
Cyber Resilience for SMEs

- Conformity assessment procedure based on internal control (based on module A)

- provided that harmonized standards or common specifications are fully applied

- EU-type examination procedure (based on module B) followed by conformity to EU-type based on internal production control (based on module C)

- Conformity assessment based on full quality assurance (based on module H)

- (where available) European cybersecurity certification schemes

at assurance level at least '**substantial**'

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

NASK

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.

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

Important products with digital elements – Class II

SECURE
Cyber Resilience for SMEs

- EU-type examination procedure (based on module B) followed by conformity to EU-type based on internal production control (based on module C)
- Conformity assessment based on full quality assurance (based on module H)
- (where available) European cybersecurity certification schemes

at assurance level at least '**substantial**'

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

NASK

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.

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

Critical products with digital elements

SECURE
Cyber Resilience for SMEs

Only where a European cybersecurity certification scheme is not available

- EU-type examination procedure (based on module B) followed by conformity to EU-type based on internal production control (based on module C)
- Conformity assessment based on full quality assurance (based on module H)

- (where available) **European cybersecurity certification schemes**

at assurance level at least '**substantial**'

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

NASK

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.

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

Free and open-source software

Applies only to important products classes I and II

- Conformity assessment procedure based on internal control (based on module A)
- EU-type examination procedure (based on module B) followed by conformity to EU-type based on internal production control (based on module C)
- Conformity assessment based on full quality assurance (based on module H)
- (where available) European cybersecurity certification schemes

Funded by the European Union

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.

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

Conformity assessment procedures

Funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

NASK

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.

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

Harmonised standards

SECURE
Cyber Resilience for SMEs

Presumption of conformity

Products with digital elements that meet the relevant harmonised standards enjoy a presumption of conformity with the essential requirements of the CRA.

Translation the CRA requirements into technical specifications

Harmonised standards translate the essential requirements of the CRA into specific, technical, and repeatable measures.

Formal standardisation request

Standards are developed based on a formal standardisation request. The European Commission issued a standardisation request encompassing 41 standards supporting the CRA. These include both horizontal and vertical standards.

Horizontal standards

Horizontal standards ensure a common approach for all products. Their goal is to ensure consistency of requirements across different product types.

Vertical standards

Vertical standards address specific product categories. These standards target important and critical products and provide a presumption of conformity.

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

NASK

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.

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

Harmonised standards

SECURE
Cyber Resilience for SMEs

„Important" and "critical" products

Priority is given to the development of standards for "important" and "critical" products. Standardization prioritizes products posing a higher security risk.

Voluntary

The use of standards is voluntary – the CRA does not require mandatory use of harmonized standards, but without them, the manufacturer may lose the ability to use self-assessment. For "critical" products, the involvement of a notified body is required.

Easier and faster process

Standards make the conformity assessment process easier and faster. The use of harmonized standards automates some CRA requirements and reduces the amount of technical evidence required.

Possibility of development

Additional standards may be developed as needed. In addition to the 41 standards from the initial application, further standards may be developed to support the practical implementation of CRA requirements.

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

NASK

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.

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

Conformity assessment procedure based on internal control

- The manufacturer independently conducts a full product conformity assessment, without the involvement of a notified body.
- The manufacturer bears full responsibility for the product's conformity, both before placing the product on the market and during market surveillance.
- The manufacturer performs a risk analysis, identifying all hazards associated with the product and the requirements it must meet.
- The manufacturer determines the means to ensConformity assessment procedure based on internal control (based on module A)ure compliance, for example, by applying harmonized standards or other technical specifications.
- The manufacturer creates complete technical documentation, including a product description, analysis results, diagrams, design data, and test reports.
- The manufacturer implements internal production control procedures to ensure repeatability and compliance of each product with the documentation.

Funded by the European Union

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.

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

Conformity assessment procedure based on internal control

- The manufacturer independently performs the necessary tests and inspections, confirming the product's compliance with the essential requirements.
- After completing the conformity assessment, every product must be marked with the CE symbol by the manufacturer.
- The manufacturer prepares and signs the EU Declaration of Conformity, confirming compliance with all requirements of the legislation.
- The documentation and declaration must be kept for the required period (usually 10 years) and made available to market surveillance authorities upon request.

Funded by the European Union

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.

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

EU-type examination and Conformity to type based on internal production control

SECURE
Cyber Resilience for SMEs

- Under Module B, a notified body conducts an EU-type examination of a representative product sample, assessing its technical documentation, design, and security-relevant characteristics to confirm compliance.
- Module B results in the issuance of an EU Type Examination Certificate, which confirms that the examined type meets requirements and enables the manufacturer to proceed with production only of products conforming to this approved type.
- Module C requires the manufacturer to ensure that every product placed on the market conforms exactly to the approved type certified under Module B, using internal production control to maintain cybersecurity compliance throughout manufacturing.
- No notified body is involved in Module C, provided that the manufacturer maintains strict conformity with the type assessed in Module B.
- Once conformity with the requirements is ensured, the manufacturer affixes the CE marking and issues the EU Declaration of Conformity, confirming that both the assessed type (Module B) and all produced units (Module C) meet the requirements.

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

NASK

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.

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

Conformity based on full quality assurance

SECURE
Cyber Resilience for SMEs

- The manufacturer implements a comprehensive quality system covering design, production, and final inspection, ensuring conformity with essential requirements.
- A notified body assesses and approves the entire quality system, including periodic audits and ongoing supervision.
- The manufacturer ensures that product design and production processes consistently meet the required standards, carrying out tests and controls within the approved system.
- The manufacturer issues a Declaration of Conformity and affixes the CE marking together with the notified body's identification number.
- The notified body monitors continued compliance, overseeing the whole production process to ensure each unit remains conformant.

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

NASK

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.

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

SECURE
Cyber Resilience for SMEs

National Use Cases

Carmelo Dimauro

Project Lead

NC3/LHC (NCC Luxembourg)

Work Package 5:
SECURE the existent: national use cases

The objective of the National Use Cases Work Package (WP) is to facilitate the **collection, sharing, and dissemination of best practices and use cases** related to Cyber Resilience Act (CRA) compliance at the national level.

Funded by the European Union

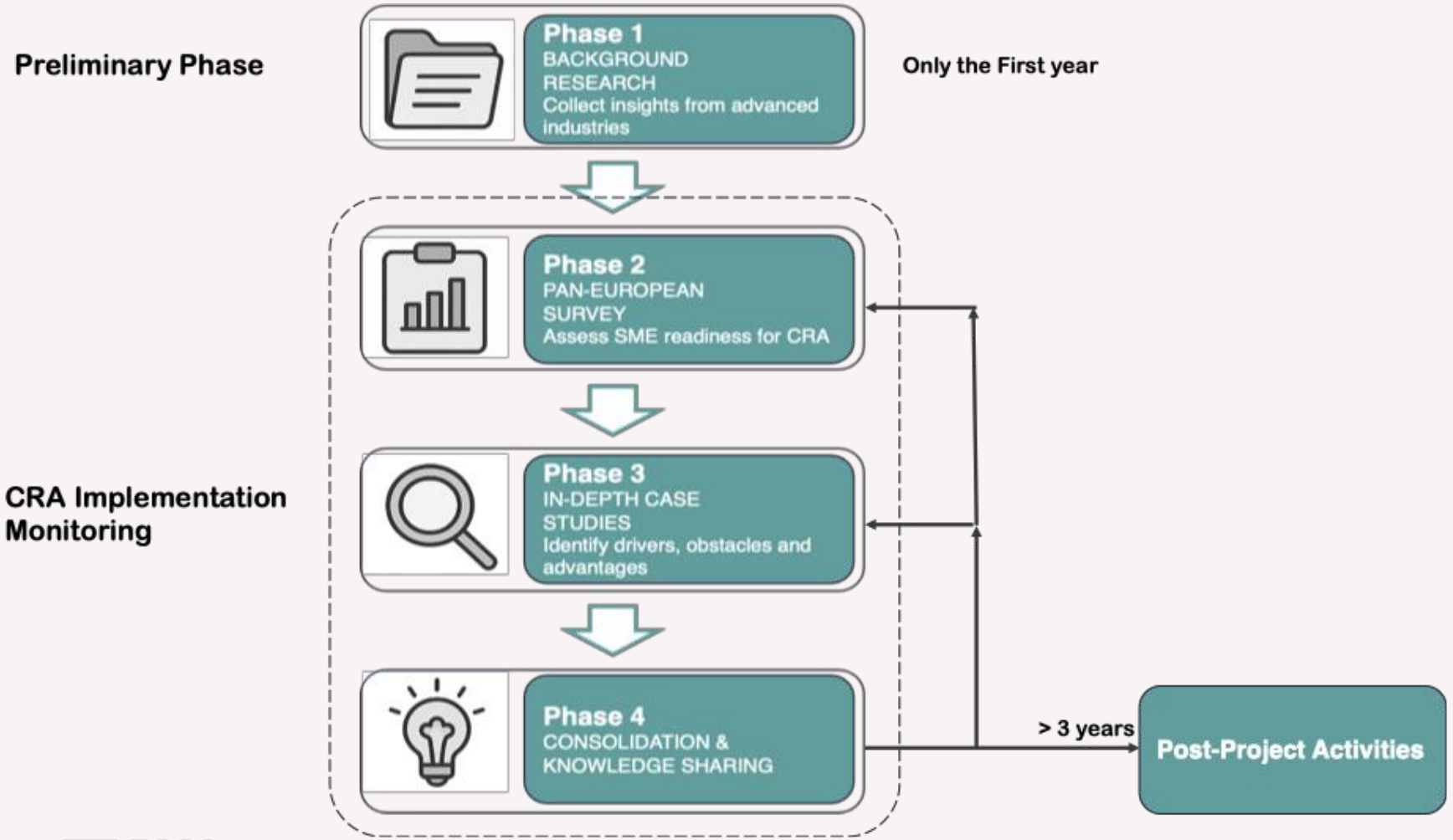
Work Package 5:
SECURE the existent: national use cases

By gathering insights and examples of successful CRA compliance strategies from various SMEs, this WP aims:

- to provide **valuable guidance** to refine the evaluation criteria of the calls implemented under WP2, as well as

- to **share relevant inputs** for SMEs during the project and roadmap for future developments.

Workflow of the strategy



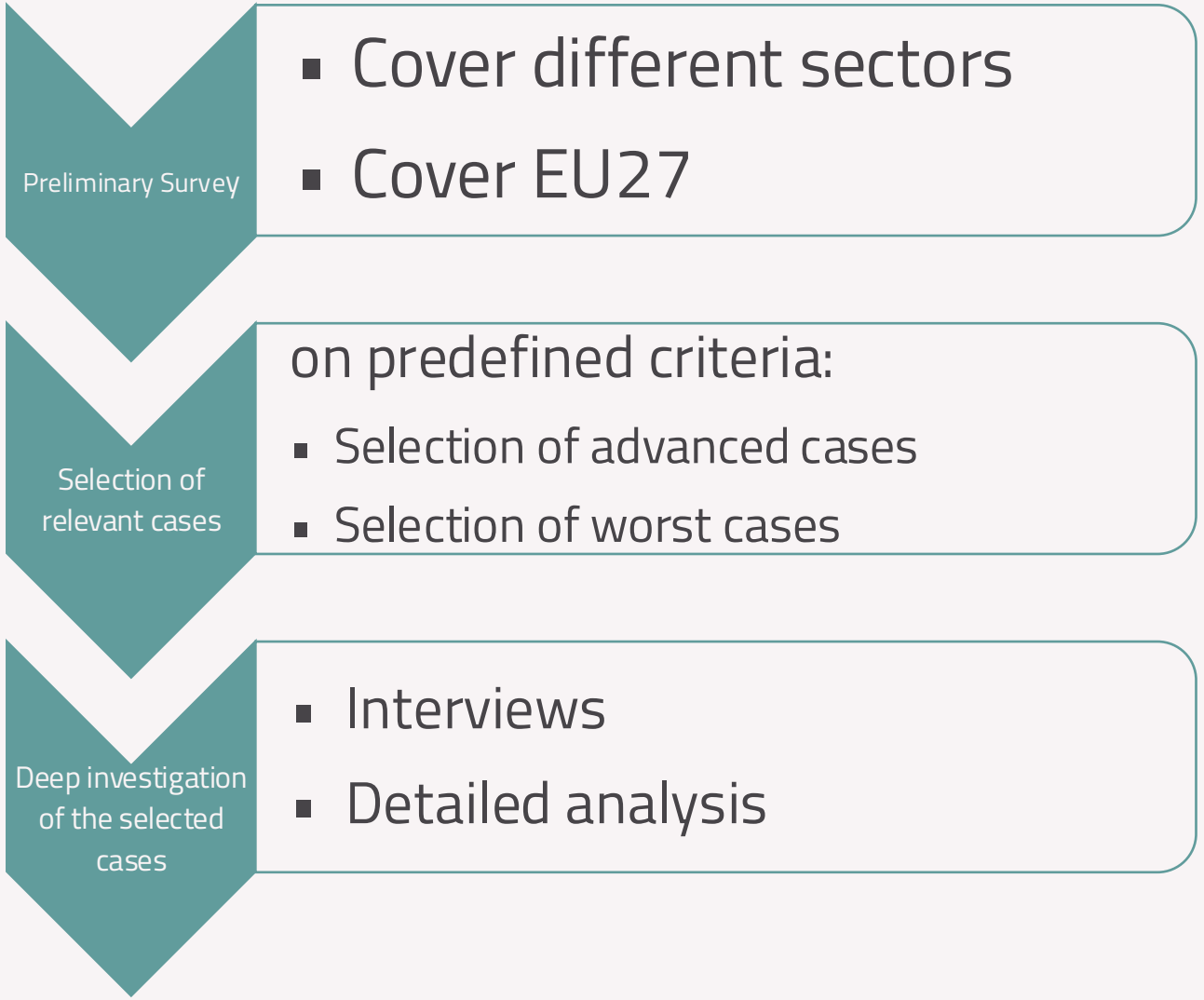
Funded by the European Union

Complexity

SECURE
Cyber Resilience for SMEs

Level of Maturity / Readiness

Technical gaps



Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CRA is interesting because it blends:

Mandatory compliance

+

market-driven competition.

If companies treat CRA as "*legal paperwork*," they will struggle.

If they integrate it into product engineering processes, adoption will accelerate and create competitive advantage.

Funded by the European Union

Key factors (likely) influencing the adoption of CRA

SECURE
Cyber Resilience for SMEs

Coercive Drivers

- Market access (CE marking requirement)
- Fines and enforcement credibility
- National authority oversight

Strategic Drivers

- Brand reputation
- Competitive differentiation
- Export harmonization

Market Drivers

- Procurement requirements
- B2B supply chain pressure
- Insurance requirements

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Identify Main Obstacles

SECURE
Cyber Resilience for SMEs

CRA adoption barriers are very specific:

- Lack of secure development lifecycle
- No internal vulnerability disclosure process
- No SBOM generation capability
- Supply chain opacity
- SME resource constraints
- Uncertainty about harmonized standards
- Notified body capacity bottlenecks

WP5 should test whether companies fear:

- Compliance cost
- Engineering rework
- Time-to-market delays

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Learning from other experiences

Other sectors operate under strict cyber-regulatory or safety-critical frameworks:

1. Aviation (DO-178C, DO-326A)
2. Medical devices (MDR, IVDR, IEC 62304)
3. Automotive (UNECE WP.29, ISO 21434)
4. Railways (TSI, CENELEC EN 5012x standards)
5. Energy (NIS2-related frameworks, IEC 62443)
6. Industrial automation / OT systems

Despite differing domains and terminology, CRA and sectoral standards share the same underlying principles:

- Structured lifecycle management
- Risk-based approach
- Documentation and traceability
- Rigorous verification and validation
- Continuous post-market monitoring and update
- Stakeholder confidence.

Funded by the European Union

Time Schedule

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dic
Phase 1 – Background Research: Context Setting and Benchmarking												
Analysis of sectorial standards												
Meeting & Interviews												
Analysis of the outcomes												
Dissemination				**Reporting & paper**								
Phase 2 – Pan-European Survey: Monitoring SME Readiness and Implementation												
Design												
Testing												
Launch												
Analysis												
Dissemination											**Survey Report**	
Phase 3 – In-Depth Case Studies: Understanding Drivers, Barriers, and Benefits									**Interviews**			
Phase 4 – Consolidation and Knowledge Sharing: From Evidence to Action												
											1st year Report	
Dissemination				**FIC**		**GRC Summit**				**Cyber week**		

Funded by the European Union

SECURE
Cyber Resilience for SMEs

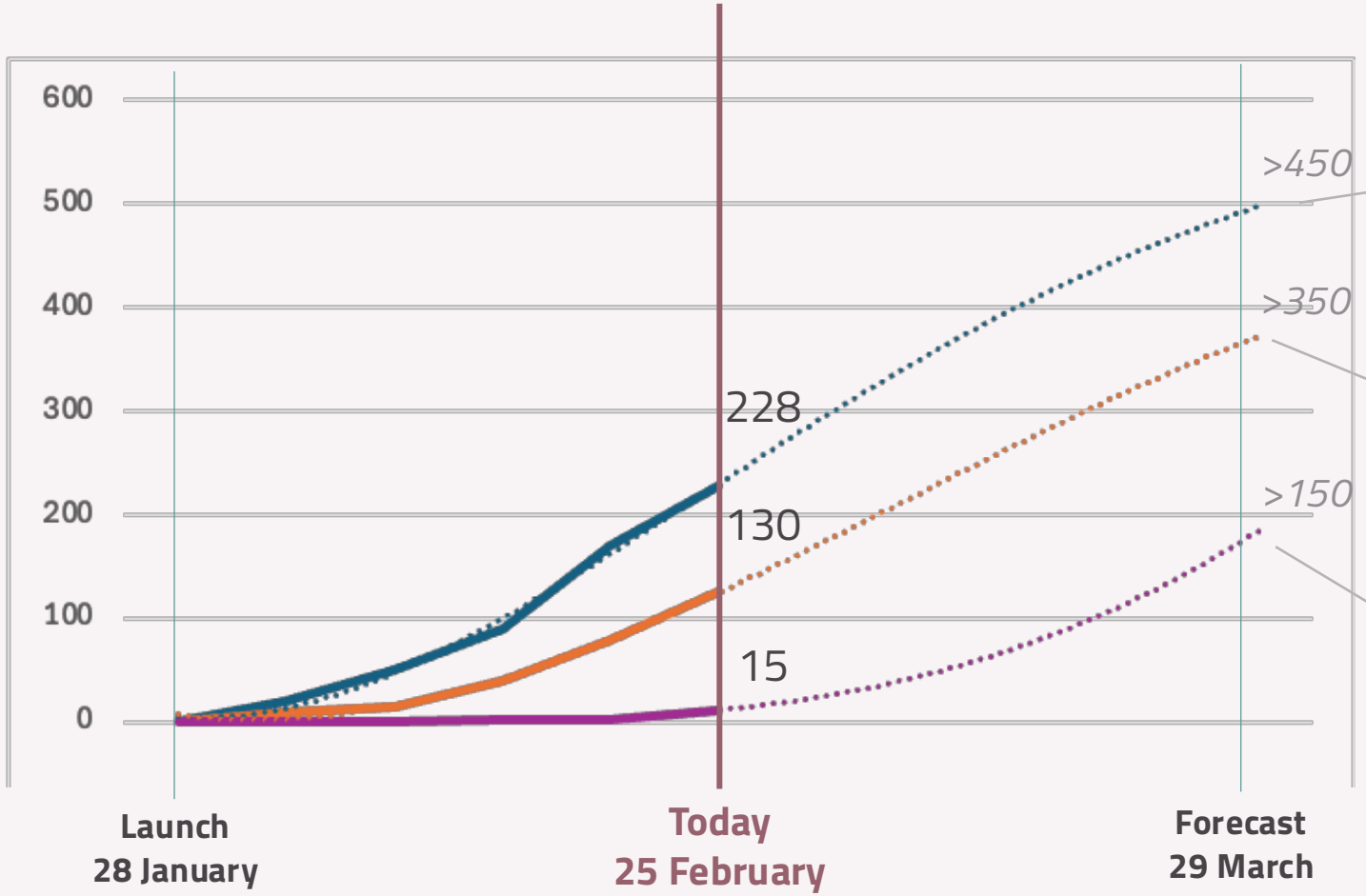
1st Open Call - Guidelines and Application Process

Alessandro Calabrese

Head of Advisory & Training

Cyber 4.0

N. of Applicants & Applications



Company Profile Created

- Actual = 228
- Forecast >450

Registered Companies

- Actual = 130
- Forecast >350

Proposals Submitted

- Actual = 15
- Forecast >150

The peak in application volume is typically expected in the 10 days leading up to the call deadline

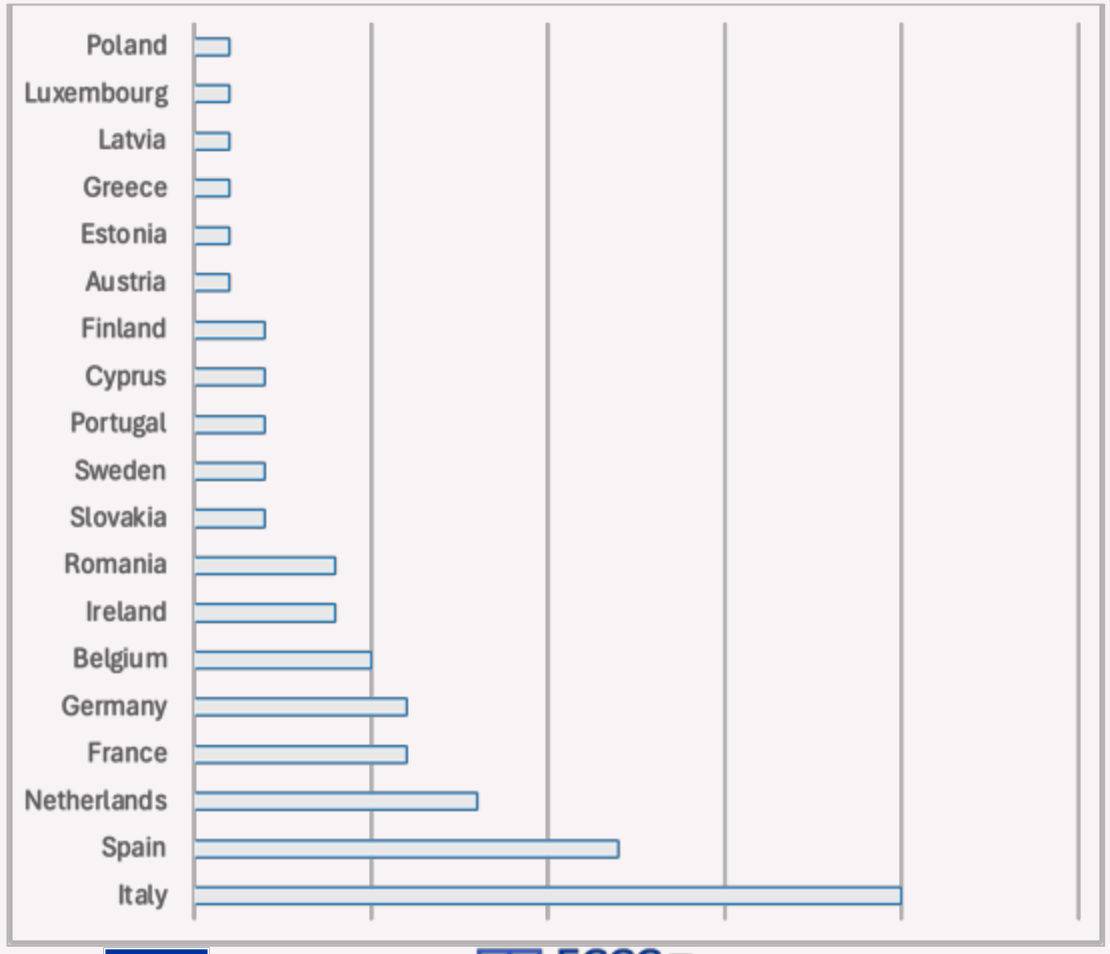
MAX FUNDABLE COMPANIES =166

Funded by the European Union

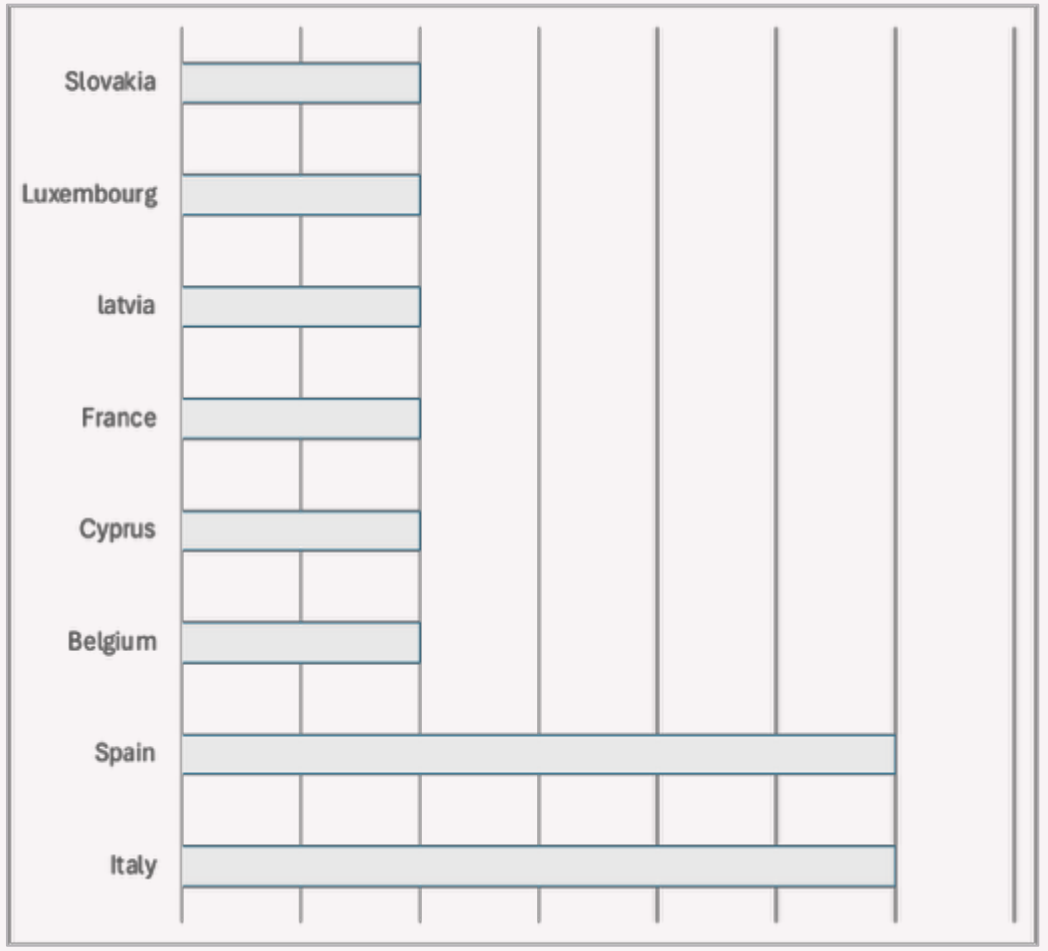
Country Overview

SECURE
Cyber Resilience for SMEs

ACTIVE ACCOUNTS



SUBMITTED PROPOSALS



Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SECURE
Cyber Resilience for SMEs

INTRODUCTION

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

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

1st Open Call General Information

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

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** - *max 80% of direct costs; only for the shared cost corresponding to the actual rate of use during project duration*
- **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

ELIGIBILITY REQUIREMENTS

Call Eligibility Requirements

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

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**

SECURE
Cyber Resilience for SMEs

APPLICATION & IMPLEMENTATION PROCESS

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

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 HASE 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

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	**0,00 €**

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 2 - Writing a SECURE lump sum proposal

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

Phase 2 - Eligible Costs - General definition

THE COSTS MUST BE

reasonable, justified	*identifiable and verifiable*	*complied with the applicable national law*
actually incurred	*incurred during the period of implementation*	*referred to one or more relevant budget category*
necessary for the project implementation	*entered in the budget as eligible costs*	*recorded in the beneficiary's accounts*

If any of the above conditions is not met, the cost is not eligible and will be rejected

Funded by the European Union

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 - Equipment costs in pills

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

Reference: DEP AGA Article 6.2.C.2

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	

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.

Final Ranking

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

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

Implementation Phases

SECURE
Cyber Resilience for SMEs

PHASE 5
Initial CRA Maturity Assessment

COMPLETE THE CRA MATURITY ASSESSMENT ON PLATFORM

PHASE 6
Implementation & Technical Report

To Do – Implement & Upload Documents:

- Complete the proposed project
- Upload the Technical Report
- Upload other necessary evidences

PHASE 7
Implementation Assessment, Payment & Attestation

CHECK PLATFORM AND E-MAIL FOR EV.CO. INTEGRATION REQUEST

GET FUNDED!

COMPLETE SURVEY & DOWNLOAD ATTESTATION

More details will be provided during next webinars

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

Partnership with other EU Projects

CYBERSTAND.eu Project

Nicholas Ferguson

Senior Manager & Coordinator of CYBERSTAND.eu - Trust-IT Services

Funded by the European Union

ECCC

SECURE
Cyber Resilience for SMEs

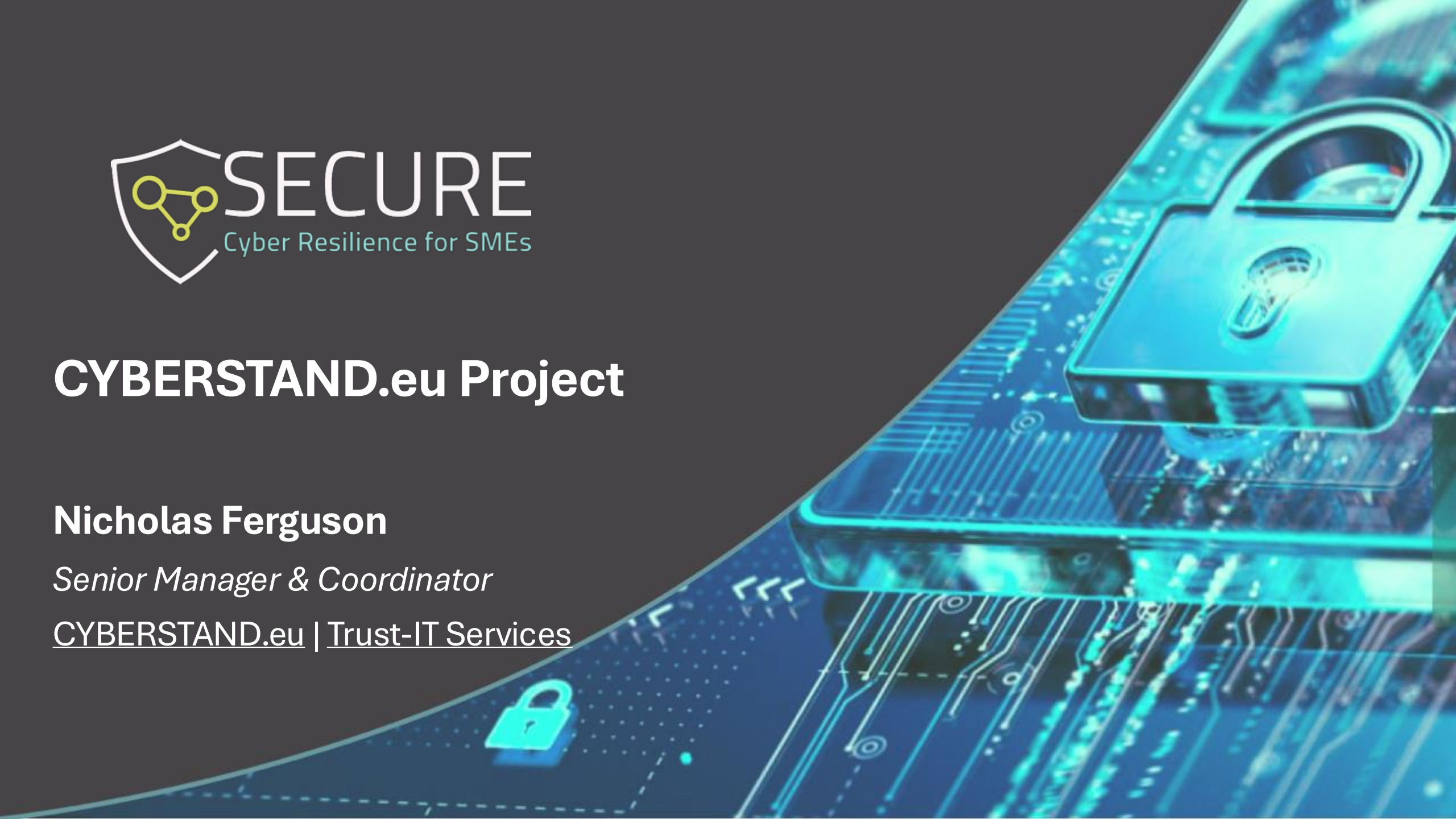
SECURE
Cyber Resilience for SMEs

CYBERSTAND.eu Project

Nicholas Ferguson

Senior Manager & Coordinator

CYBERSTAND.eu | Trust-IT Services



For Compliance, Read **Security, Trust & Confidence** – Standards, Tools and Funding for the CRA

SECURE Dissemination DAY
Rome, Italy
25th February 2026

Nick Ferguson,
Senior Manager,Trust-IT Services
Coordinator of Cyberstand.eu

www.cyberstand.eu

Funded by the European Union

Cyberstand.eu in a Nutshell

CYBERSTAND.eu

Mission: Engaging And Supporting EU Experts In Cybersecurity Standardisation Activities

OBJECTIVES

Objective 1: Deliver a coherent and engaging series of events and publications to establish an inclusive community on the CRA

Objective 2: Establish a facility dedicated to support EU experts contributing to standardisation efforts, in EU an Int'l cybersecurity standardisation fora.

Objective 3: Foster the development on harmonised standards, in conformity with the Cyber Resilience Act (CRA).

Objective 4: Contributing to implementation of European Values and sustainability of the CRA.

FUNDING FOR STANDARDS

- 100+ EU Experts funded to contribute to CRA standards (€1,500,000 assigned)
- Contribution to multiple standardisation Work Items
- Increased participation of SMEs in CRA standardisation activities

CRA GUIDES

- Standards implementation guides for SMEs
- Risk assessment guide
- Vulnerability handling guide
- Standardisation reports from EU experts
- Prioritisation of CRA Work Items

SYNERGIES UNLOCKED

- CRA Cluster formed with 12 projects
- 3 Community groups on technology, standardisation and outreach
- Community-related synergies with NCCs
- Direct dialogue with SME and Start-up associations

BROADER PERSPECTIVES

- CRA Implementation for SMEs and micro-enterprises
- Member state preparedness and guidance
- Interplay with other EU legislation
- International mapping and exploring alignment

EVENTS AND ENGAGEMENT

- 3 Annual Impact Events
- 6 CRA SME Workshops
- 6 CRA Standards Training Sessions
- 12 Webinars & Training Sessions
- 2 public consultations
- Outreach at 18+ third party events

EU projects

SMEs & Start-ups

Cybersecurity Organisations, including ECCC, NCCs, ENISA

Vertical Industries Representatives

Policy Makers, MS Representatives, and SDOs

CONTRIBUTIONS TO CRA STANDARDS

Co-funded by the European Union

ECCC

CYBERSTAND.eu

168 **Submitted Applications**
From SSP1 to SSP9

78 **Funded Contributions**
For a total amount of **€ 1,175,507**

55% Contributions awarded to **Small and Medium Enterprises**

Gender
35% Female
65% Male

Addressing Standardisation Requests

36	13	52
Horizontal standards for security requirements	Horizontal standards for vulnerability handling requirements	Vertical standards for security requirements

Type of Contributions

49	25	4
Long term	Medium Term	Short Term

Contributions to **Technical Committees**

- 45 **ETSI for Cyber Security and its standardisation activities** (ETSI TC CYBER)
- 38 **Cybersecurity and Data Protection** (CEN/CENELEC JTC 13)
- 8 **Semiconductors and Trusted Chips Implementation** (CENELEC TC 47X)
- 7 **Personal identification and related personal devices with secure element** (CEN TC 224)
- 7 **Industrial-process measurement, control and automation** (CENELEC TC 65X)

Nationality

- 12 France
- 11 Germany
- 9 Italy
- 9 Spain
- 8 Croatia

CYBERSTAND.eu
Engaging & supporting EU experts in Cybersecurity Standardisation activities

Current Funding Opportunities

Funding

- Ensure the CRA standards are SME-friendly and easily implemented
- Address key areas where SMEs may struggle with CRA compliance.
- Continuous evaluation and quick starts

Topics

- *SME Guidance for standards implementation*
- *Readability/usability checks of standards*
- *Standard implementation use cases*

Funding types*

- Review a draft standard (Up to €3,000)
- Create an SME guide (Up to €10,000)

Deadline – 10th March

https://cyberstand.eu/10th-specific-service-procedure-sme-perspective

*Applicants **individuals or natural persons** residing **in European Member States**

Vertical standards

- *17 Standalone & embedded browsers*
- *19 SW that searches malicious SW*
- *26 Operating systems*
- *27 Routers, modems & switches*
- *30 ASIC and FPGA with security-related functionalities*
- *31 Smart home general purpose virtual assistants*
- *32 smart home products with security functionalities*
- *33 connected toys covered by Directive 2009/48/EC*
- ***34 wearable products with health monitoring***
- *35 hypervisors and container runtime systems*
- ***40 smart meter gateways within smart metering systems***

Operational Technologies

- *20b VPN*
- *21b Network management systems*
- *22b SIEM systems*
- *25b Physical and network interfaces*
- *27b Routers, modems & switches based on EN IEC 62443*
- *36b Firewalls & intrusion detection & prevention*

CYBERSTAND.eu
Engaging & supporting EU experts in Cybersecurity Standardisation activities

Tools, Guides, Training and Funding

EC-Funded Projects Supporting CRA Implementation

Certification, Tools & Alignment with EU Legislation

CRACoWi
Cybersecurity Compliance Made Easy

Simplifying CRA compliance with automated tools for cybersecurity certification and assessments.

TrustBoost

Enhancing cybersecurity compliance and certification across the EU and aligning with major EU regulations.

Tools, Methodologies and Training for Compliance

CONFIRMATE

Open-source tools to facilitate and automate compliance with the CRA.

CURIUM

CRA compliance tools and services automation and capacity building.

OCCTET

Open-source toolkit to automate the compliance process for Free and Open Source Software (FOSS).

CRA - AI
CYBER RESILIENCE ACT ARTIFICIAL INTELLIGENCE

AI-powered platform built to guide product companies through the full CRA conformity journey.

CYBERFORT

Compliance tools for SMEs, documentation automation, and open-source accessibility promotion.

CYBERGUARD
A POWERED DEFENSE

Strengthening Europe's cybersecurity through AI-driven defence, collaborative intelligence, and real-world validation.

cracy
CRA made easy

Methodologies and tools to facilitate the documenting process to ensure compliance with the CRA.

OSCRAT
Open-Source Cyber Resilience Act Tools

Empowering SMEs with open-source tools for compliance with the CRA for PDEs.

Funding SME Compliance

SECURE
Cyber Resilience for SMEs

Open calls and resources for SMEs to comply to the CRA

Funding & Support for Standardisation

CYBERSTAND.eu

Funding contributions to develop standards for the CRA.

Co-funded by the European Union
ECCC

CYBERSTAND.eu

Engaging & supporting EU experts in Cybersecurity Standardisation activities

CRA Standards Unlocked – EU Tour

Speakers

- European Commission
- National Cyber Security Centre
- National Standardisation Body
- European Standardisation Organisations
- SME & Industry associations
- EU-Funded projects
- Standardisation experts

Topics

- CRA overview & update
- Standards deep dives
- Compliance tools, training & funding
- Best practices
- Implementation stories
- Benefits for SMEs

Jan 2026

Feb 2026

Next Stops

- Barcelona, 26th March
- Paris, April 2026 date TBC
- Stockholm, 4th May 2026
- Malta, 21st May 2026
- Bucharest, June – date TBC
- Berlin, October – date TBC
- Sophia Antipolis, October – date TBC

CYBERSTAND.eu

Thank you!

Nicholas Ferguson (Coordinator)
n.ferguson@trust-itservices.com

www.cyberstand.eu

Funded by the European Union

Cyberstand.eu: The Essentials

- **Objective**: Engaging & supporting EU experts in cybersecurity standardisation activities
- **Type**: Coordination & Support Action 101158521
- **Duration**: June 2024 – May 2027
- **Budget**: €2,999,999.09
- **Call**: Deployment actions in the area of cybersecurity (DIGITAL-ECCC-2023-DEPLOY-CYBER-04)

Cyberstand.eu Partners

Trust-iT services communicating to markets
COMMpla Communication Platforms and Online Solutions
ECSO European Cyber Security Organisation
European DIGITAL SME Alliance
ETSI
cen
CENELEC

The EU Cyber Resilience Act (CRA)

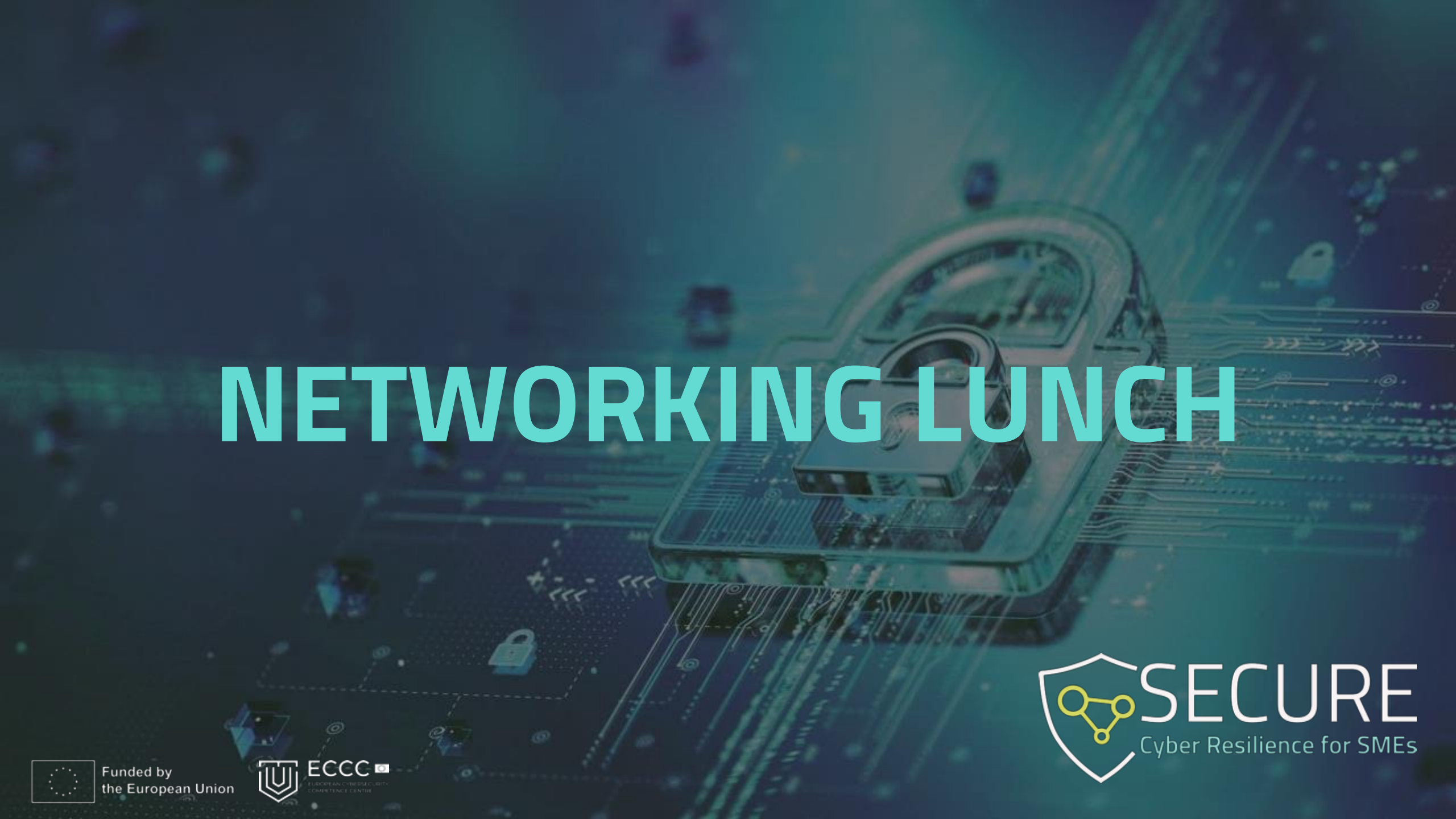
- *"New EU cybersecurity rules ensure safer hardware and software."*
- One of the most significant pieces of regulation to come from Europe in recent years.
- Impact will extend well-beyond Europe's borders.
- Companies large and small, whether based in Europe or wanting to export into Europe will have to comply.
- CRA compliance is a market entry requirement
- Clear stakeholder engagement and guidance is a must for the successful implementation of the CRA

Funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

SECURE
Cyber Resilience for SMEs

NETWORKING LUNCH



Funded by the European Union

ECCC

SECURE
Cyber Resilience for SMEs

SECURE

Cyber Resilience for SMEs

Dissemination Day Rome

25th February 2026

9.30 - 14.00 (CET)

Hybrid Event

Funded by the European Union

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

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