FORUM 2025
CYBER 4.0

ROMA TRE Aula Magna Rettorato
4 - 5 Giugno 2025

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Secure Project

Financial Support to European mSMEs for CRA Compliance

Andrea Margheri
Capo Divisione Progetti Industriali e Tecnologici, ACN

Con il patrocinio di:

Ministero delle Imprese e del Made in Italy

Sotto l'alto patrocinio del Parlamento europeo

Finanziato dall'Unione europea
NextGenerationEU

Hosted by:
ROMA TRE
UNIVERSITÀ DEGLI STUDI

Cyber Resilience Act (CRA)

Essential **cybersecurity requirements** for the **design and development** of **products with digital elements** (hardware and software) as well as obligations for all **economic operators** in the value chain.

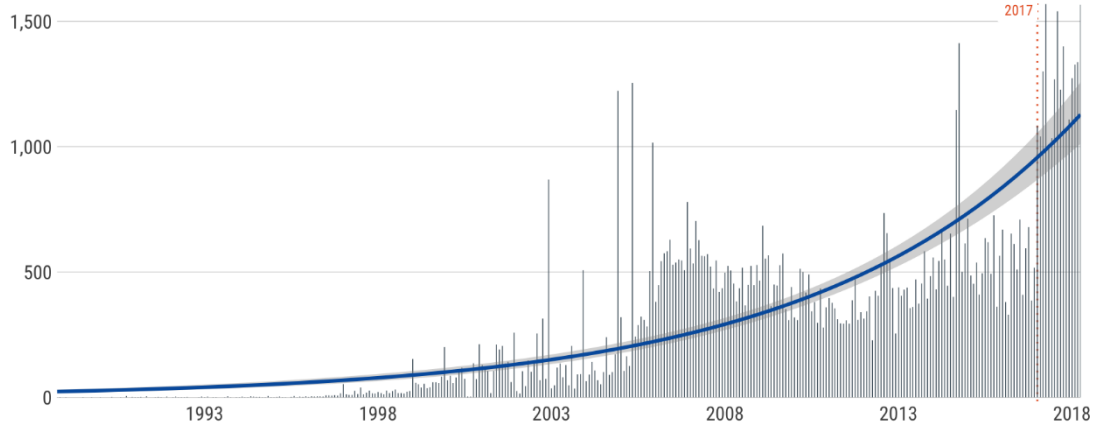


Figure 1: **Number of CVE (Common Vulnerabilities and Exposures) per month**

Political agreement in December 2023
Regulation not yet adopted.

SMEs in the Scope of CRA

Manufacturers of Products with Digital Components
e.g. manufacturing of electronic component, computer and peripheral equipment, communications equipment and consumer electronics

Providers of Tools and Solutions for CRA Compliance
e.g. IT consulting, cybersecurity services, compliance software solutions, data protection and privacy services, training and educational services.

Other Well-Justified Categories in Line with CRA
e.g. technology distribution and importation, open-source software development, regulatory advisory services, cybersecurity standardisation bodies, digital infrastructure services

Funded by the European Union

Key information about cybersecurity of italian SMEs

- ACN recognizes the importance of protecting SMEs for strengthening supply chains.
- ACN supports SMEs by facilitating technological transfer through Digital Innovation Hubs, involving them in R&D activities, promoting the uptake of cybersecurity certification and through targeted awareness raising campaigns.

99% of Italian businesses are SMEs.

51 out of100, cybersecurity maturity of Italian SMEs

+60% cyberattacks increase in Italy between 2018 and 2022

83% of Italian SMES use digital tools to support their business processes

>50% of SMEs operates within critical supply chains, being particularly vulnerable to cyberattacks

13% of Italian SMEs reported suffering at least one cyber breach in the last four years

Funded by the European Union

SECURE Project - Overview

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Main Objectives

- **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 f. upskilling & 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

€ 30.000
Maximum amount of co-funding (50% of the total project costs) to be granted to each SME

Partner

Coordinator

ACN – Agenzia per la Cybersicurezza Nazionale

Consortium Partners

NCC Centrul Național de Coordonare Cybersecurity România

LHC Luxembourg House of Cybersecurity

CYBER 4.0 Cybersecurity Competence Center

NCC-BE Belgium Cybersecurity Coordination Centre

NASK .pl

incibe_ Instituto Nacional de Ciberseguridad

INDUSTRIE 4.0 Austria

Affiliated Partners

virtual vehicle

TECHHOUSE

ideare ideas & research hub

salzburgresearch

PROFACTOR

TU WIEN Technische Universität Wien

External Contributors

- NCCs or relevant national authorities of all EU27 and EEA/EFTA countries.
- The EDIH network.

ECCC

EDIH European Digital Innovation Hubs Network

FORUM 2025
CYBER 4.0

ROMA TRE Aula Magna Rettorato
4 - 5 Giugno 2025

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

SECURE Stakeholders

The Role of NASK

Paweł K. Kostkiewicz
Director for Certification, NASK

Con il patrocinio di:

Ministero delle Imprese e del Made in Italy

Sotto l'alto patrocinio del Parlamento europeo

Finanziato dall'Unione europea
NextGenerationEU

Hosted by:
ROMA TRE
UNIVERSITÀ DEGLI STUDI

The Role of NASK - PL

NASK will lead WP 1

- Task 1.1 (by M6) – Stakeholders mapping
- Task 1.2 (by M9) - Stakeholders needs & preferences analysis (including collection of platform requirements) – Led by Cyber 4.0
- Task 1.3 (throughout the project) - Continuous stakeholder engagement

  → in close collaboration with ECCC, NCCs Network, EDIHs network

Contributor to all WPs

- Strongly involved in Task 6.4 on 'Contribution to standardisation effort' – Led by ACN – aimed at analysing existing standards which may contribute to the adoption of the CRA requirements for SMEs.
- NASK-PL to ensure the engagement of stakeholders to align with the standards identified through participation in standardisation activities and dissemination of outcomes.

Cyber Resilience Act Obligations

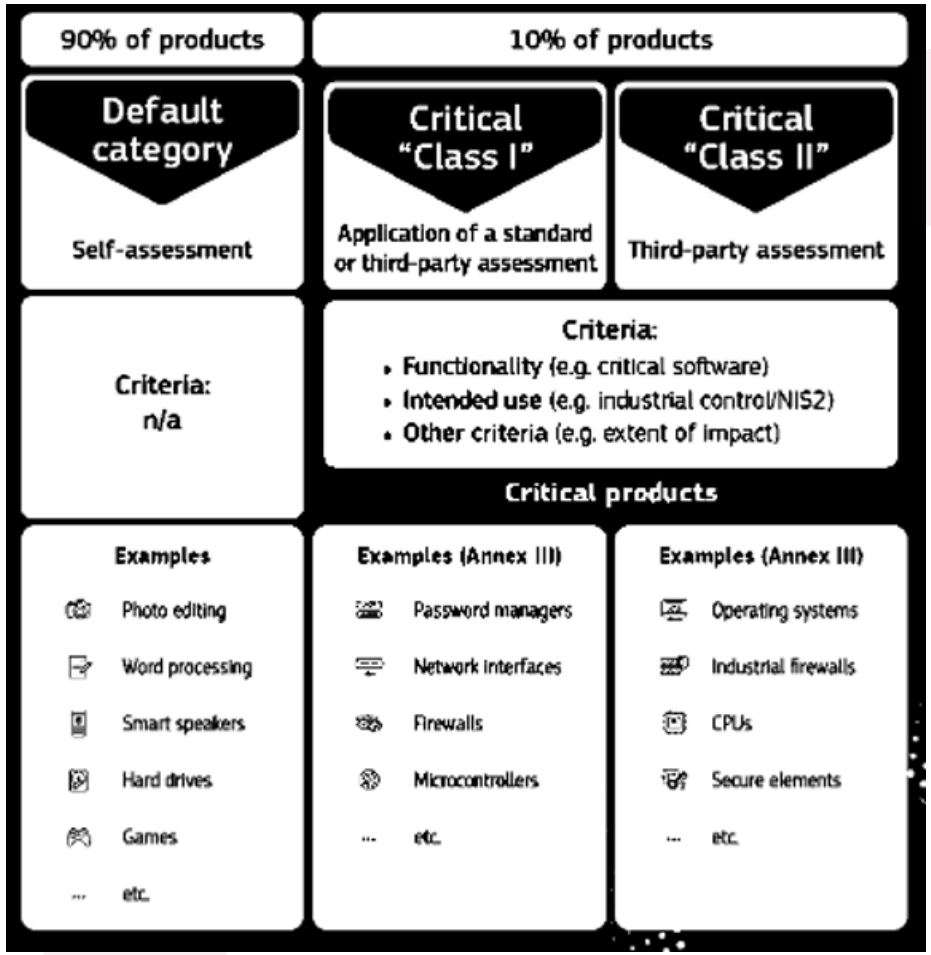
Defining SECURE Fundable Services

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

CRA Obligations

- Cybersecurity is taken into account in **planning, design, development, production, delivery and maintenance phase**
- All cybersecurity risks are **assessed and documented**
- **Security updates** to be made available to users for the time the product is expected to be in use
- Ensure that product's vulnerabilities are handled effectively for the duration of the **support period (5 years)**
- Clear and **understandable instructions** for the use of products with digital elements
- **Report** actively exploited **vulnerabilities and incidents**



Funded by the European Union

CRA stakeholders

FORUM 2025 CYBER 4.0

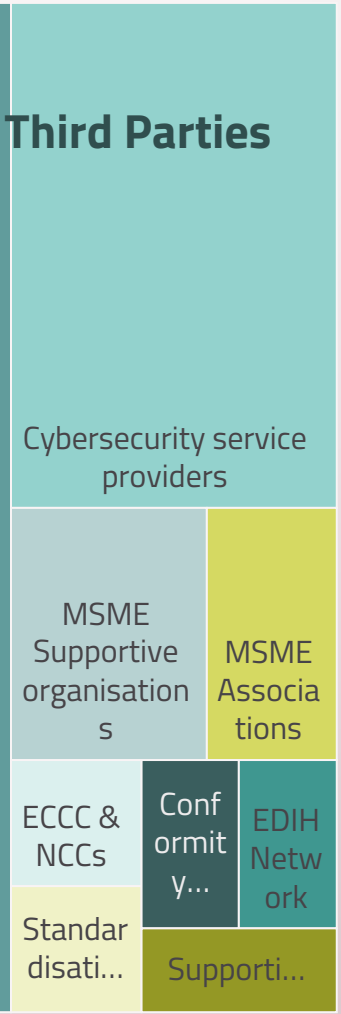
CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Economic Operators

- MANUFACTURERS
- Software developers
- Importers & Distributors
- Resellers

Eonomic Operators (~production)

Third Parties



- Eonomic Operators (~production)
- Cybersecurity service providers
- MSME Associations
- MSME Supportive organisations
- ECCC & NCCs
- Standardisation bodies
- Conformity assessment bodies
- EDIH Network
- Supportive projects

FORUM 2025
CYBER 4.0

ROMA TRE Aula Magna Rettorato
4 - 5 Giugno 2025

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

SECURE – Open Calls & Cascade Funding Management

Alessandro Calabrese
Head of Advisory and Training, Cyber 4.0
alessandro.calabrese@cyber40.it

Con il patrocinio di:

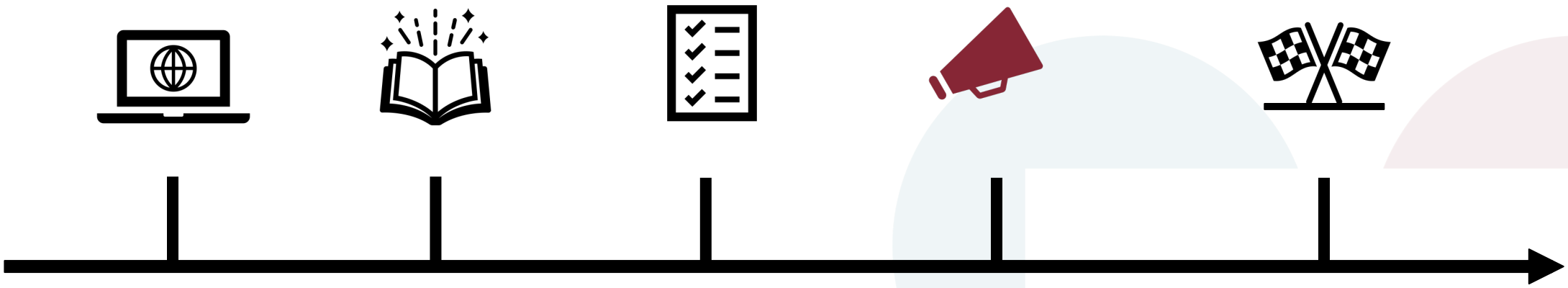
Ministero delle Imprese e del Made in Italy

Sotto l'alto patrocinio del Parlamento europeo

Finanziato dall'Unione europea
NextGenerationEU

Hosted by:
ROMA TRE
UNIVERSITÀ DEGLI STUDI

Project Timeline Draft



September
Launch of Central Open Repository

September
Guidelines and Materials for SMEs CRA compliance

October
Open Calls Application Guidelines / FSTP Platform Launch

~November~
First Call Opens

January
First Call closes

3 CALLS PROGRAM

First Call: From November 2025 → **Second Call:** From April 2026 → **Third Call:** From November 2026

The Role of Cyber 4.0 and WP2

*Open Call & Cascade Funding **Management** & **Platform***

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

CYBER 4.0

WP2 LEADER

Open Calls Management

Platform Development

ideare ideas & research hub

IDEARE SRL

Cyber 4.0 Affiliated Entity

WP2 OBJECTIVES

- Definition of **processes functionalities** and roles to handle FSTP;
- **Provide NCCs with a platform** to manage pre-submissions and check requirements
- **Provide SMEs with a friendly and secure tool** to send submissions and to monitor the status of applications for funding;
- **Provide to internal and external operators a platform** to examine and rank submissions, and to monitor outcomes;
- **Management of Open Calls** through the platform for an effective FSTP.

THE OPEN-CALLS **PLATFORM**

Designed for:

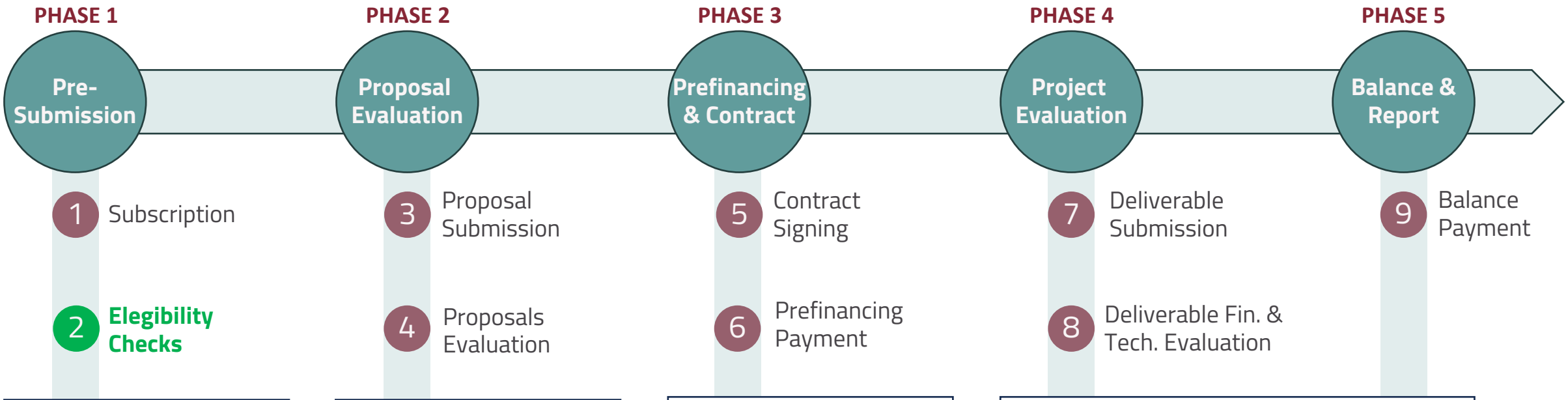
- Applicant Companies -
- NCCs -
- Consortium Members -
- Technical Evaluators -
- Financial Evaluators -

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SECURE Cyber Resilience for SMEs

Open Calls Submission Process Phases



Eligibility
- Only EU individual mSMEs can be funded
- Status of the beneficiary
- Ownership and Control

Proposals
- Uploadable through the **platform**
- Estimated **Costs** Definition
- Formal and Technical **Evaluation**

Prefinancing
- Will be asked through the **platform**
- Will cover a **percentage** of the fundable costs

MAX FUNDING RATE

=

50% of the total Project Cost

(The maximum fundable amount will be defined upon publication of the guidelines)

FORUM 2025
CYBER 4.0

ROMA TRE Aula Magna Rettorato
4 - 5 Giugno 2025

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

SECURE – Open Calls Platform

Alberto Garinei
Chief Scientific Officer, IdeaRe

Con il patrocinio di:

Ministero delle Imprese
e del Made in Italy

Sotto l'alto patrocinio
del Parlamento europeo

Finanziato
dall'Unione europea
NextGenerationEU

Hosted by:

ROMA TRE
UNIVERSITÀ DEGLI STUDI