SECURE
Cyber Resilience for SMEs

# SECURE: rafforzare la resilienza cyber delle PMI europee

Matteo Lucchetti

*Direttore Operativo ,Cyber 4.0*

Andrea Margheri

*Capo della Divisione Progetti Industriali e Tecnologici del Servizio Programmi Industriali, Tecnologici e di Ricerca (ACN)*

4 giugno 2026, Roma

# Cyber Resilience Act – Un recap

## Obiettivo del CRA

- Introdurre requisiti obbligatori di cybersecurity per tutti i ***Products with Digital Elements*** (hardware, software e relative soluzioni remote).

## Riguarda Produttori, Importatori, Distributori

## Principali obblighi

- Security-by-design e gestione del rischio lungo tutto il **ciclo di vita del prodotto**.
- Gestione delle vulnerabilità e rilascio di **aggiornamenti di sicurezza** per il periodo di utilizzo previsto
- **Notifica** di:
  - vulnerabilità attivamente sfruttate;
  - incidenti gravi che impattano sicurezza prodotto.

## Valutazione della conformità

- **Categoria standard** → autovalutazione.
- **Prodotti importanti** (es. OS, router, firewall) → standard armonizzati o valutazione di terze parti.
- **Prodotti critici** (es. smart card, secure elements) → possibile certificazione dedicata.
- **Open Source**: generalmente autovalutazione, salvo categorie critiche.

## Tempistiche chiave

- Piattaforma unica di reporting ENISA entro **sett 2026**.
- Compliance attesa entro **dicembre 2027**

Funded by the European Union

# SECURE Project Overview

SECURE
Cyber Resilience for SMEs

| SECURE | | |
|---|---|---|
| Sostenere le **PMI** europee, con particolare attenzione alle micro e piccole imprese, per **rafforzare le loro capacità nella cybersicurezza** e **supportare l'attuazione del Regolamento sul CRA**. | | |
| **INFORMAZIONI GENERALI** | | |
| **Budget totale: 22 mln €** | Finanziato da DIGITAL-DEPLOY-CYBER-06-STRENGTHENCRA | **Durata: 3 anni** |
| **Budget FSTP (open call): 16.5 mln €** | | **Data d'inizio: 1 Gennaio 2025** |
| **OBIETTIVO GENERALE** | | |
| • **Gestione delle Open Call** garantendo una valutazione imparziale e un monitoraggio trasparente del finanziamento a cascata<br>• **Garantire la consapevolezza, l'accessibilità e il coinvolgimento delle PMI europee** nei finanziamenti a cascata<br>• **Stabilire risorse per la compliance al CRA**; **piattaforma** online come principale strumento per l'upskilling e capacity building<br>• Svolgimento di attività di **formazione e aggiornamento delle competenze** degli stakeholder per garantire la conformità al CRA<br>• **Promozione della condivisione della conoscenza** e facilitazione dei casi d'uso di conformità al CRA<br>• Contributo alla **standardizzazione dell'applicazione del CRA** attraverso il coinvolgimento di organismi europei e internazionali | | |

**CONSORZIO** *(5 NCC e 3 organizzazioni)*

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

*Inoltre*

**AFFILIATED ENTITY**

ideare ideas & research hub

**External Contributors**

ECCC

NCC o autorità nazionali competenti pertinenti di tutti i Paesi dell'UE27 e EEA/EFTA

# Open Call e implementazione CRA

Il progetto SECURE ha mantenuto un **costante allineamento con le fasi di implementazione del Cyber Resilience Act** (CRA), seguendo in modo proattivo gli elementi introdotti in ciascuna fase.

Questo approccio ha permesso di **anticipare requisiti e priorità emergenti**, anche **in vista delle future open call** e dell'**evoluzione dei framework di certificazione e compliance**.


Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

# Open Call e implementazione CRA (2/2)

SECURE
Cyber Resilience for SMEs

**11 Dicembre 2025**

*"Adopt an implementing act specifying technical descriptions of categories of products with digital elements"*
*Art. 7 (4)*
+
*"Adopt delegated acts specifying terms and conditions for delaying the dissemination of notifications"*
*Art. 14 (9)*

**11 Giugno 2026**

*"Conformity assessment bodies notifications provisions apply "*
*Art. 71 (2)*

**11 Settembre 2026**

*"Reporting obligations concerning actively exploited vulnerabilities and severe incidents affecting the security of products with digital elements apply"*
*Art. 71 (2)*

**Q4 2026**

Delegated Act specifying the presumption of conformity for the European Cybersecurity Certification scheme on Common Critera (EUCC) with the CRA

**11 Dicembre 2026**

*"Ensure a sufficient number of bodies to perform conformity assessments, thus avoiding obstacles to market entry "*
*Art. 35*

*"Prepare and submit a technical report on trends on emerging cybersecurity risks"*
*Art. 17 (3)*

**10 Dicembre 2027**

*"The Cyber Resilience Act fully applies "*
*Art. 69 (3)*

**11 Dicembre 2027**

*"Requirements for products with digital elements placed on the market before December 2027 apply if substantially modified"*
*Art. 69 (2)*

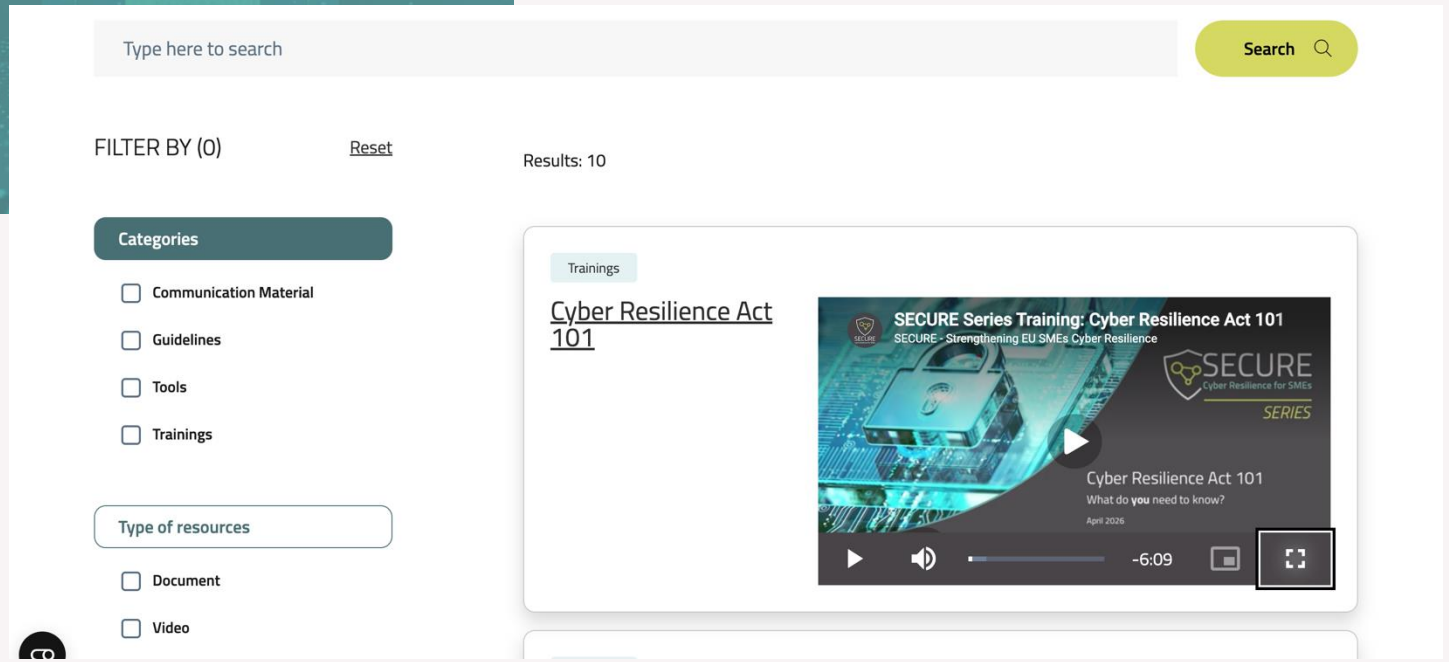
1st Open Call

2nd Open Call

3rd Open Call

Commissione Europea | Operatori economici | Stati Membri | ENISA | Produttori/Rivenditori

# Repository Cyber Resilience Act e Progetto SECURE


Funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

**Maggiori informazioni:** SECURE Website

# Open Call per le PMI europee

SECURE
Cyber Resilience for SMEs

SECURE prevede un meccanismo di finanziamenti a cascata attraverso open call dedicate alle **micro, piccole e medie imprese** dell'Unione Europea

**Almeno 2 open call** verranno pubblicate per cofinanziare progetti volti a **migliorare la conformità al CRA**, **rafforzare le pratiche di cybersicurezza** e **promuovere un approccio armonizzato** alla resilienza in tutta l'UE.

La **prima call** è stata lanciata a **Gennaio 2026**, la seconda verrà lanciata nella seconda metà del 2026. Le mPMI avranno la possibilità di ricevere fino a €30.000 (a copertura del 50% dei costi di progetto) per realizzare progettualità di CRA compliance della durata di sei mesi .

Per la prima Open Call, il budget di **5 milioni di euro** verrà assegnato ai progetti selezionati; i restanti **11,5 milioni di euro** saranno destinati alle **prossime Open Call**.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

# Punti chiave della 1° Open Call

SECURE sta raccogliendo risultati molto positivi: la prima Open Call ha registrato **oltre 250 candidature** ricevute, superando le aspettative. Questa forte partecipazione conferma la rilevanza dell'iniziativa e l'elevato interesse da parte delle PMI in tutta Europa.

## Risultati chiave

- **Proposte pervenute da 28 Paesi** *(26 paesi UE con l'eccezione di Malta + paesi non-UE: Islanda e Regno Unito)*
- **91 proposte sottomesse in Italia** – risultando il paese con la partecipazione più ampia
- Forte coinvolgimento delle mPMI anche in **Germania (28 proposte)** e **Spagna (27 proposte)**

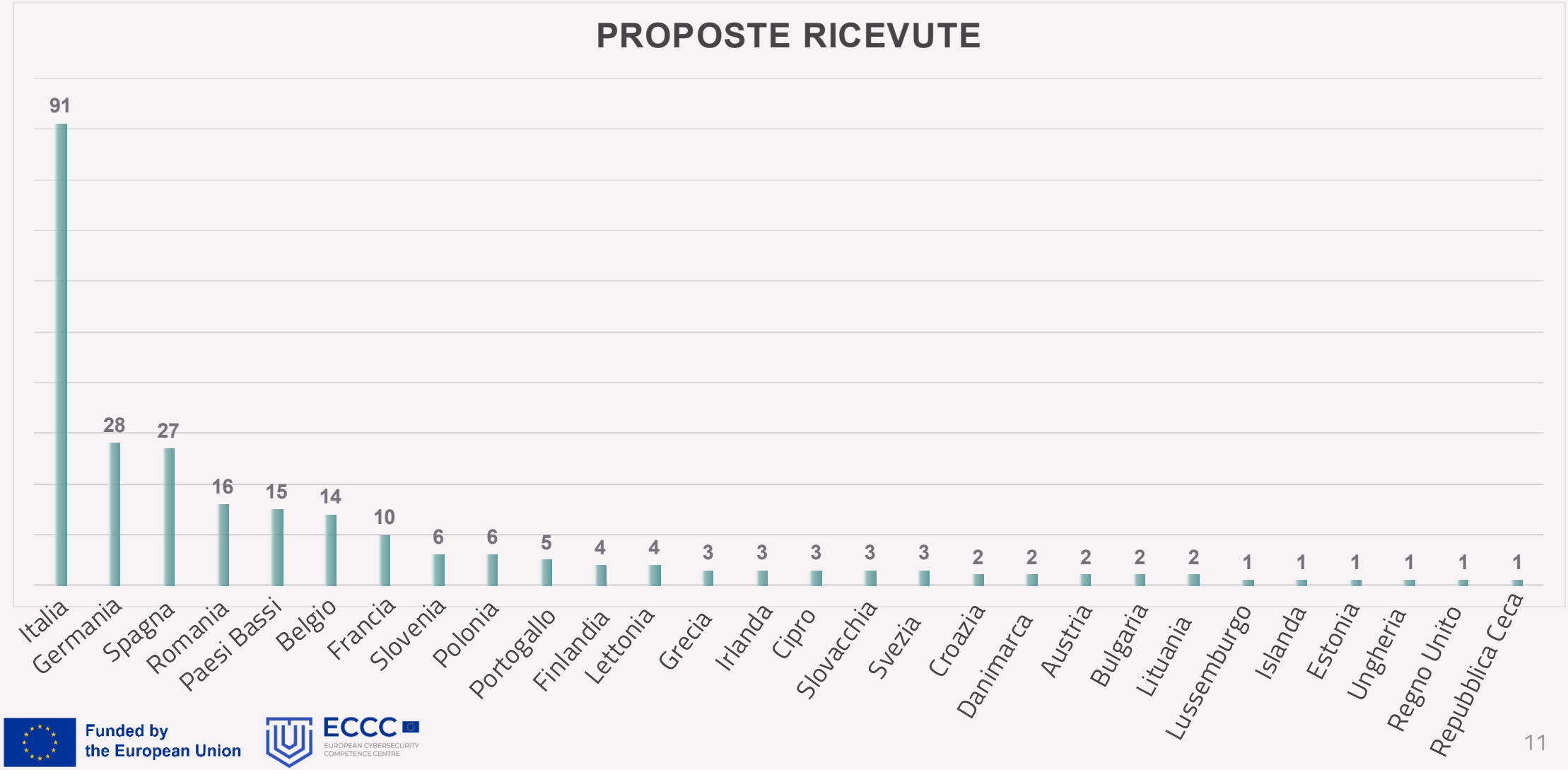
## Stato attuale

- Si è **conclusa la valutazione tecnica** delle proposte in capo ad un team di esperti (**Evaluation Committee**), avvenuta in modo da garantire imparzialità, correttezza, equilibrio, trasparenza e oggettività.
- Le proposte che hanno superato la prima fase di valutazione sono state trasmesse agli **NCC** dei relativi Paesi, incaricati di svolgere le verifiche di ammissibilità e gli **Ownership Control Assessment.**
- Per le prossime Open Call ci si aspetta una **partecipazione più equilibrata e omogenea da parte di tutti gli Stati europei.**



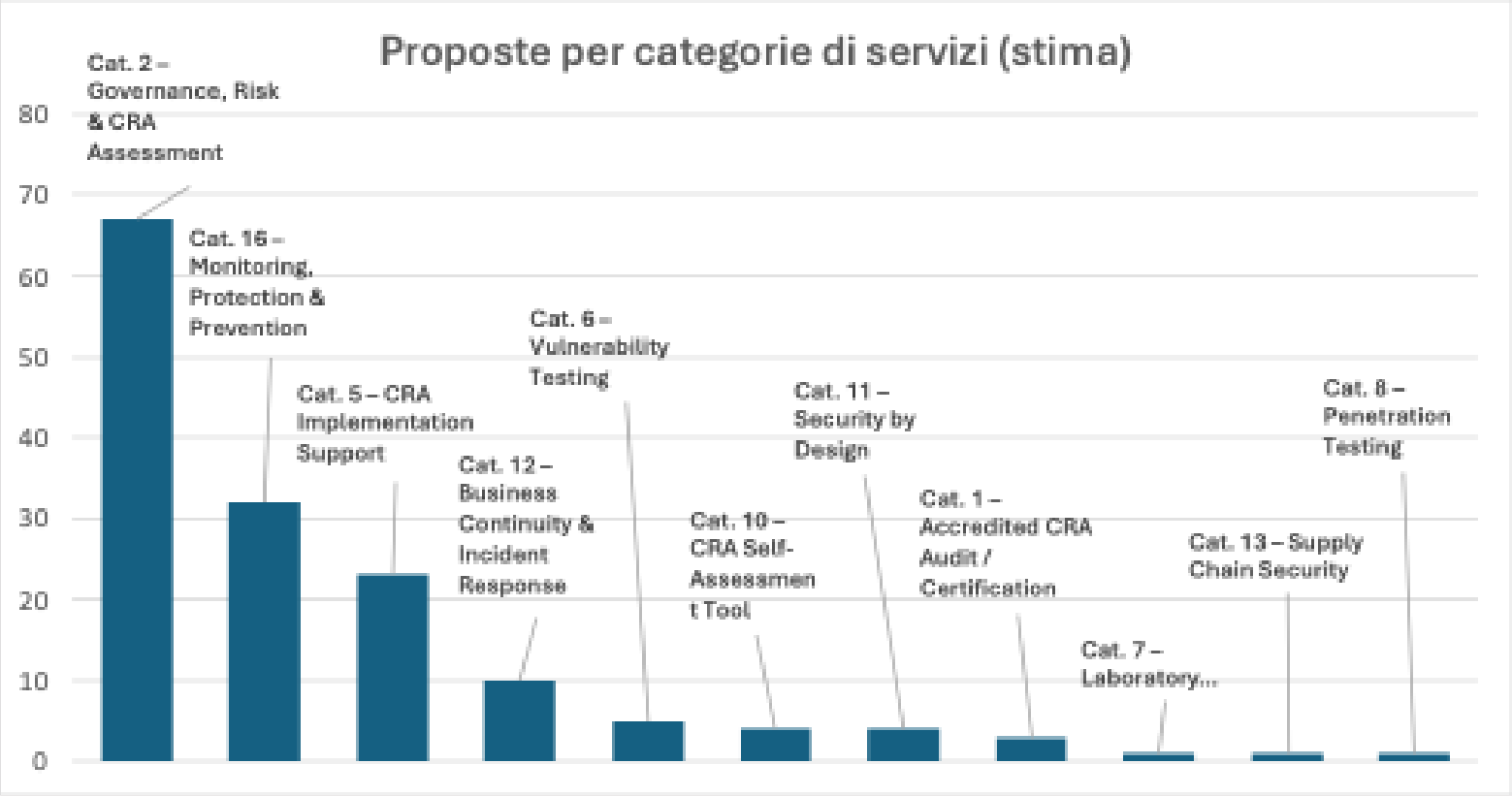
Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

# 1° Call : Proposte ricevute per Paese




Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

# 1° Call : Proposte ricevute per categorie servizi




Quasi una proposta su due riguarda attività preliminari di:

- gap assessment
- maturity assessment
- analisi dei requisiti CRA;
- governance;
- risk management

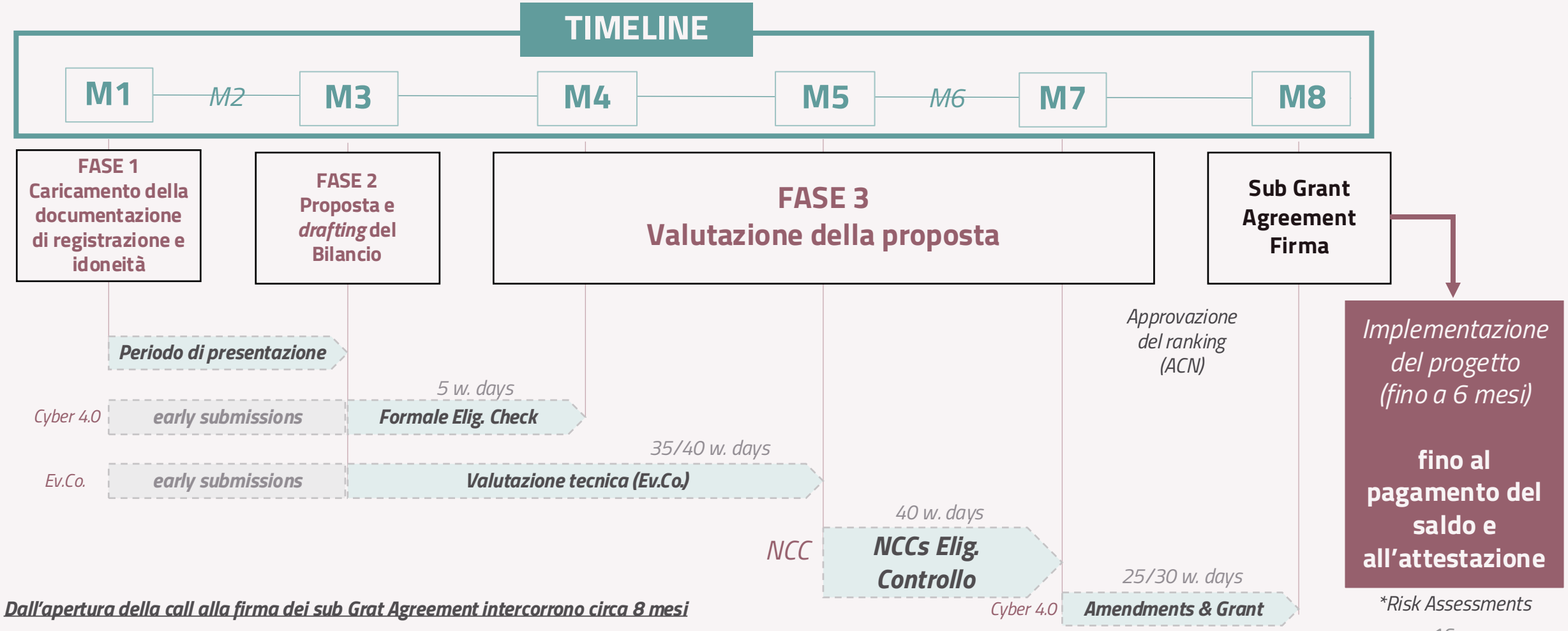
Bassa richiesta di certificazioni, laboratori, come era atteso

- **Le PMI europee sono ancora nella fase di comprensione del CRA  più che di compliance operativa**
- **Il CRA viene percepito come un problema organizzativo più che tecnologico**

Funded by the European Union

# Le fasi e i passaggi delle Open Call

SECURE
Cyber Resilience for SMEs




***Dall'apertura della call alla firma dei sub Grat Agreement intercorrono circa 8 mesi***

*Risk Assessments



Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

# Prossime Open Call per le mPMI europee

SECURE
Cyber Resilience for SMEs

- **SECURE** continua il dialogo con la Commissione EU per sostenere un **approccio coerente tra Bandi alle mPMI e timeline di implementazione del CRA**
- **Requisiti generali per le future Open Call**

→ **Requisiti** relativi all'ambito CRA per i candidati: i candidati devono operare in un settore o svolgere attività che rientrano nell'ambito del CRA e dei relativi framework normativi, oppure dimostrare la volontà di farlo.

→ **Attività ammissibili**: saranno considerati solo i progetti finalizzati al raggiungimento della conformità al CRA.

**Stakeholder di interesse:**


**Produttori**


**Distributori**


**Importatori**


**Autorizzato Rappresentanti**


**Operatori che apportano modifiche sostanziali**

**Maggiori informazioni sul lancio del prossimo bando saranno comunicati attraverso il sito internet di progetto e i social media:**

SECURE Website

Funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

# Grazie mille!

**Website:** [www.secure4sme.eu](http://www.secure4sme.eu)

Contact Mail: info@secure4sme.eu

Linked In

Youtube

Funded by the European Union

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

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