# Rafforzare le capacità di cybersecurity delle PMI europee in linea con i requisiti e gli obblighi CRA

## Strengthening cybersecurity capacities of European SMEs in line with CRA requirements and obligations

**TOPIC ID**:
DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STRENGTHENCRA

**Ente finanziatore:**
Commissione europea
Programma Europa digitale

**Obiettivi ed impatto attesi:**
Obiettivo:
L'obiettivo di questo tema è sostenere le PMI europee, con particolare attenzione alle micro e piccole imprese, a rafforzare le loro capacità di cybersecurity e a sostenere l'attuazione della proposta di regolamento sulla Cyber Resilience Act (CRA).
Ambito di applicazione:
In sinergia con le altre azioni lanciate nell'ambito di questo WP, che svilupperanno strumenti di conformità per il CRA, l'azione dovrebbe distribuire sovvenzioni di finanziamento a cascata alle PMI europee, con particolare attenzione alle micro e piccole imprese, pur rimanendo aperta ad altre parti interessate, per sostenere il raggiungimento della conformità ai requisiti e agli obblighi derivanti dal CRA.
I richiedenti sono incoraggiati a identificare le categorie di beneficiari del finanziamento a cascata, tra cui almeno le seguenti:
• Produttori di prodotti con componenti digitali, compresi gli sviluppatori di software.
• Fornitori di strumenti e soluzioni che facilitano l'adempimento degli obblighi CRA.
• Altre categorie ben giustificate in linea con il CRA (ad esempio, distributori, importatori, comunità open-source).
Per ogni categoria di stakeholder identificata, deve essere elaborata una serie di attività dedicate, tenendo in considerazione le esigenze specifiche dei consumatori target, degli utenti commerciali e di altri stakeholder rilevanti.
Il progetto proposto deve includere azioni che affrontino i seguenti aspetti:
• Azioni di sensibilizzazione, divulgazione e altre azioni di coinvolgimento delle parti interessate con particolare attenzione al finanziamento a cascata delle PMI europee, con particolare attenzione alle micro e piccole imprese.
• Gestire un processo di invito aperto per distribuire finanziamenti a cascata, compresa la valutazione imparziale delle proposte e il monitoraggio dell'attuazione delle sovvenzioni.
• Creare una piattaforma aperta che fornisca collegamenti a risorse relative al CRA che il progetto proposto stesso raccoglierà o svilupperà o che saranno disponibili da fonti esterne, sostenendo la creazione e l'aggiornamento della comunità. Ciò include, ad esempio, un sito web dedicato al repository centrale per consentire un facile reperimento di risorse interne ed esterne, linee guida passo-passo, strumenti di

conformità, materiali di formazione, implementazioni di codice libero e open-source e altre risorse rilevanti per ottenere la conformità CRA. Ciò dovrebbe includere, tra l'altro, gli strumenti acquistati a questo scopo nell'ambito del presente programma di lavoro.
• In stretto coordinamento con la Cybersecurity Skills Academy dell'UE, svolgere attività di formazione e aggiornamento delle parti interessate per raggiungere la conformità CRA, ovvero organizzare workshop, sessioni di formazione ed eventi, redigere linee guida, sostenere azioni per facilitare l'interazione tra le PMI europee, compresa la stesura di relazioni o altro materiale che discuta l'attuazione dei requisiti di conformità CRA e promuovere la consapevolezza, anche contribuendo ai pertinenti documenti degli organismi di standardizzazione, ad esempio attraverso una prospettiva settoriale e informata dalle esigenze delle aziende sul campo.
• Facilitare e condividere le migliori pratiche e i casi d'uso della conformità CRA.
• Contribuire agli sforzi di standardizzazione, come appropriato, considerando le attività di standardizzazione europea e internazionale che sono direttamente rilevanti per l'implementazione del CRA.
I terzi che ricevono sovvenzioni devono, in particolare:
• Impegnarsi in test, individuare e risolvere le vulnerabilità, produrre documentazione, effettuare valutazioni di conformità e implementare altre misure necessarie per conformarsi al CRA.
• Partecipare a workshop, sessioni di formazione ed eventi che facilitino l'interazione tra le PMI europee, con particolare attenzione alle micro e piccole imprese, per discutere e implementare la conformità alle CRA.
• Contribuire agli sforzi del progetto proposto per raccogliere le esigenze e le prospettive delle PMI verso i prodotti di standardizzazione relativi al CRA.
La priorità dovrebbe essere data alle soluzioni disponibili all'uso gratuito o a quelle basate su software libero e open-source (FOSS), sia nella fase di creazione della piattaforma aperta che in quella di distribuzione delle sovvenzioni a cascata.
Queste attività dovrebbero essere svolte in stretto coordinamento e, ove possibile, in collaborazione con il Centro europeo di competenza per la cibersicurezza (ECCC), la rete dei Centri nazionali di coordinamento (NCC), la rete degli European Digital Innovation Hubs (EDIHs), altri enti europei e nazionali competenti in materia di cibersicurezza e altri progetti del presente programma di lavoro.
Si raccomanda vivamente il coinvolgimento operativo degli NCC nell'attuazione e nella gestione di tali azioni.
Si prevede di finanziare una sola proposta attraverso questo tema. I progetti proposti devono prevedere almeno il 75% del budget da distribuire per le sovvenzioni di finanziamento a cascata.
Questa azione prevede la creazione di una piattaforma centrale che funga da punto di riferimento e che permetta quindi l'interazione tra i fornitori di servizi essenziali e di infrastrutture critiche, nonché altri attori, in merito alle loro misure di sicurezza informatica e alle possibili vulnerabilità. Anche le terze parti che ricevono finanziamenti si impegneranno in soluzioni per testare, rilevare e affrontare le vulnerabilità. Poiché tali informazioni potrebbero essere sfruttate da attori malintenzionati, l'entità centrale che le gestisce deve essere protetta da possibili dipendenze e vulnerabilità nella sicurezza informatica per prevenire l'influenza e il controllo stranieri. Come già osservato in precedenza, la partecipazione di entità non appartenenti all'UE comporta il rischio che informazioni altamente sensibili sulle infrastrutture di

sicurezza, sui rischi e sugli incidenti siano soggette a legislazioni o pressioni che obbligano tali entità non appartenenti all'UE a divulgare tali informazioni a governi non appartenenti all'UE, con un rischio imprevedibile per la sicurezza. Pertanto, sulla base delle ragioni di sicurezza esposte, le azioni relative a queste tecnologie sono soggette all'articolo 12, paragrafo 5, del Regolamento (UE) 2021/694.

Prodotti da consegnare:
• Sostegno finanziario alle PMI e alle altre parti interessate per la conformità alle CRA.
• Piattaforma aperta con risorse relative alle CRA (come linee guida e documenti di supporto), che fornisce supporto alla creazione di comunità e all'aggiornamento.
• Workshop, eventi, networking e scambio di esperienze delle parti interessate
• Contributi alla standardizzazione delle CRA

**Criteri di eleggibilità:**
Le domande saranno considerate ammissibili solo se il loro contenuto corrisponde interamente (o almeno in parte) alla descrizione del tema per cui sono state presentate. Partecipanti ammissibili (Paesi ammissibili)
Per essere ammissibili, i richiedenti (beneficiari ed enti affiliati) devono:
- essere persone giuridiche (enti pubblici o privati)
- essere stabilito in uno dei paesi ammissibili, ossia:
- Stati membri dell'UE (compresi i paesi e territori d'oltremare (PTOM))
- Paesi SEE (Norvegia, Islanda, Liechtenstein)
I beneficiari e gli enti affiliati devono iscriversi al Registro dei Partecipanti - prima di presentare la proposta - e dovranno essere convalidati dal Servizio Centrale di Convalida (REA Validation).
Per la convalida, sarà richiesto loro di caricare documenti che dimostrino lo status giuridico e l'origine.
Altre entità possono partecipare in altri ruoli del consorzio, come partner associati, subappaltatori, terze parti che forniscono contributi in natura, ecc.
Si ricorda che tutti i temi di questo bando sono soggetti a restrizioni per motivi di sicurezza, pertanto i soggetti non devono essere controllati direttamente o indirettamente da un Paese che non sia un Paese ammissibile. Tutti i soggetti5 dovranno compilare e presentare una dichiarazione sulla proprietà e sul controllo.
Inoltre:
- la partecipazione a qualsiasi titolo (come beneficiario, entità affiliata, partner associato, subappaltatore o destinatario di sostegno finanziario a terzi) è limitata alle entità dei paesi ammissibili
- le attività del progetto (compreso il lavoro in subappalto) devono svolgersi nei paesi ammissibili
- la Convenzione di sovvenzione può prevedere restrizioni sui DPI
Composizione del consorzio - nessuna restrizione
Il sostegno finanziario a terzi è obbligatorio in DIGITAL-ECCC-2024-DEPLOYCYBER-06- STRENGTHENCRA (Rafforzamento delle capacità di cybersecurity delle PMI europee in linea con i requisiti e gli obblighi del CRA) per le sovvenzioni alle seguenti condizioni:
- i bandi devono essere aperti, ampiamente pubblicati e conformi agli standard dell'UE in materia di trasparenza, parità di trattamento, conflitti di interesse e riservatezza

- i bandi devono essere pubblicati sul Portale dei finanziamenti e delle gare d'appalto e sui siti web dei partecipanti
- i bandi devono rimanere aperti per almeno due mesi
- se le scadenze dei bandi vengono modificate, ciò deve essere immediatamente pubblicato sul portale e tutti i candidati registrati devono essere informati del cambiamento
- l'esito dell'invito deve essere pubblicato sui siti web dei partecipanti, compresa una descrizione dei progetti selezionati, le date di assegnazione, la durata dei progetti e i nomi legali e i paesi dei beneficiari finali
- le chiamate devono avere una chiara dimensione europea.

Per il tema DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STRENGTHENCRA Rafforzare le capacità di cybersecurity delle PMI europee in linea con i requisiti e gli obblighi del CRA la durata indicativa dell'azione è di 36 mesi, ma non sono escluse altre durate.

**Contributo finanziario:**
Tipo di azione e tasso di finanziamento Sovvenzione per il sostegno a terzi - tasso di finanziamento del 100% per il consorzio, cofinanziamento del 50% da parte di terzi sostenuti
Il budget disponibile per il bando è stimato in 22.000.000 di euro.
Budget del progetto (importo massimo della sovvenzione): - Per il tema DIGITAL-ECCC-2024-DEPLOY-CYBER-06-STRENGTHENCRA Rafforzamento delle capacità di sicurezza informatica delle PMI europee in linea con i requisiti e gli obblighi del CRA: 22 milioni di euro per progetto.

**Scadenza:**
26 marzo 2024 17:00:00 ora di Bruxelles

**Ulteriori informazioni:**
**call-fiche_digital-eccc-2024-deploy-cyber-06_en.pdf (europa.eu)**