ANEXA 2 - Domeniul de aplicare CRA - Activități, servicii și bunuri eligibile

Funded by the European Union

Declarație privind finanțarea UE: Finanțat de Uniunea Europeană în baza Acordului de grant nr. 101190325. Opiniile și punctele de vedere exprimate aparțin exclusiv autorilor și nu reflectă în mod necesar poziția Uniunii Europene sau a Centrului European de Competențe în Securitate Cibernetică (industrial, tehnologic și de cercetare). Nici Uniunea Europeană, nici autoritatea finanțatoare nu pot fi considerate responsabile pentru acestea.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Disclaimer ECCC: Proiectul este sprijinit de Centrul European de Competențe în Securitate Cibernetică și de membri acestuia.

Cuprins

1 Introducere

Prezenta anexă la Ghidul primului Apel Deschis SECURE are ca scop furnizarea de orientări privind cerințele de eligibilitate legate de domeniul de aplicare al CRA pe care societățile solicitante trebuie să le îndeplinească, precum și activitățile, serviciile sau bunurile pentru care poate fi solicitată cofinanțarea.

- **Primul capitol** prezintă domeniul de aplicare al CRA , cu obiectivul de a clarifica tipurile de societăți care pot solicita finanțare. În special, activitățile principale ale societăților trebuie evaluate în raport cu tipurile de produse care intră în domeniul de aplicare al CRA .
- **Al doilea capitol** oferă o listă de activități, servicii și bunuri care pot fi eligibile pentru cofinanțare. Toate activitățile enumerate pot servi drept sursă de inspirație pentru elaborarea propunerilor de proiecte și sunt menite să consolideze nivelul de conformitate al societăților solicitante cu CRA.

La redactarea propunerilor de proiecte utilizând acest document ca referință, trebuie avut în vedere faptul că Regulamentul CRA va fi adoptat oficial de Uniunea Europeană, iar principalele sale obligații vor fi puse în aplicare de statele membre până în 2027. Din acest motiv, și în absența unor dispoziții de reglementare mai detaliate, evaluarea conformității cu cerințele de eligibilitate legate de CRA se va baza pe regulamentul propriu-zis și pe orientările oficiale disponibile în prezent.

Având în vedere stadiul actual de implementare a CRA și intenția de a sprijini cât mai multe societăți, toate propunerile din partea microîntreprinderilor și IMM-urilor care ar putea intra în sfera de aplicare a CRA vor fi considerate eligibile. Această abordare se aplică atât societăților care se încadrează în prezent în domeniul de aplicare al CRA, cât și celor care, prin dezvoltările planificate ale activității sau producției, vor intra sub incidența acestuia în viitorul apropiat.

Subcontractarea

Toate activitățile enumerate în capitolul 2 pot fi puse în aplicare fie de personalul propriu al societății solicitante, fie de un furnizor terț selectat de solicitant (de exemplu, consultanți sau furnizori de servicii). Dacă activitățile urmează să fie realizate de un furnizor/prestator, costurile aferente vor fi clasificate ca și costuri de subcontractare, care sunt considerate eligibile pentru finanțare în cadrul prezentului apel.

Alegerea furnizorului trebuie justificată prin includerea informațiilor relevante despre acesta în ANEXA 1.3 – Modelul de buget al propunerii și în ANEXA 1.1 – Modelul de propunere.

Regulile specifice privind subcontractarea sunt descrise în *ANEXA 1.2 – Ghid pentru elaborarea bugetului propunerii.*

2 Domeniul de aplicare al CRA și cerințele de eligibilitate aferente CRA

2.1 Introducere și observații preliminare

Actul privind Reziliența Cibernetică (CRA), Regulamentul (UE) 2024/2847, introduce cerințe orizontale de securitate cibernetică pentru produsele cu elemente digitale (PDE) introduse pe piața Uniunii Europene. Numai societățile ale căror activități și produse ar putea intra în domeniul de aplicare al CRA sunt eligibile pentru a aplica în cadrul acestui Apel.

Este important de subliniat că regulamentul CRA va deveni pe deplin aplicabil la 11 decembrie 2027, anumite obligații (cum ar fi obligația de a raporta vulnerabilitățile exploatate și incidentele de securitate cibernetică) urmând să intre în vigoare la 11 septembrie 2026. Până atunci, evaluarea privind încadrarea unei societăți sau a unui produs în domeniul de aplicare trebuie să rămână flexibilă și să se bazeze pe orientările actuale furnizate de Comisia Europeană și ENISA:

- Comisia Europeană – Actul privind reziliența cibernetică [1]
- ENISA – Securitatea cibernetică a produselor cu elemente digitale[2]

Prezenta anexă explică în detaliu domeniul de aplicare al CRA , identifică categoriile de produse vizate, clarifică rolul producătorilor, importatorilor și distribuitorilor și oferă exemple privind modul în care societățile pot fi afectate.

2.2 Principiile de bază ale CRA

În esenţă, Regulamentul (UE) 2024/2847 – Actul privind Reziliența Cibernetică (CRA), stabilește cerințe orizontale de securitate cibernetică pentru produsele cu elemente digitale introduse pe piața UE. Scopul său principal este de garanta că produsele și serviciile digitale sunt:[3]

- sigure prin proiectare (secure by design), cu securitatea cibernetică integrată încă din primele etape ale conceperii, dezvoltării și producției;
- reziliente la amenințările cibernetice, capabile să reziste exploatării și să se adapteze la vulnerabilitățile emergente; și
- capabile să asigure o protecție continuă pe tot parcursul ciclului lor de viață, susţinute de mecanisme securizate de actualizare și de procese de gestionare a vulnerabilităților.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02024R2847-20241120

[2]https://certification.enisa.europa.eu/publications/cyber-resilience-act-implementation-eucc-and-its-applicable-technical-elements_en https://www.enisa.europa.eu/topics/product-security-and-certification

[3] Pentru mai multe informații și clarificări detaliate, vă rugăm să consultați capitolul 5 din CRA101: Înțelegerea obligațiilor CRA; și capitolele 3 și 5 din Cadrul de evaluare metodologică a conformității al CRA.

CRA răspunde riscurilor tot mai mari asociate conectivității crescute, impunând controale obligatorii de securitate cibernetică pentru o gamă largă de produse digitale, indiferent de locul fabricării, cu condiția să fie disponibile pe piața UE.

Prin introducerea conceptului de securitate prin proiectare (security-by-design), CRA marchează trecerea de la reglementarea reactivă la cea preventivă în materie de securitate cibernetică. În loc să se bazeze pe măsuri voluntare sau pe standarde sectoriale fragmentate, CRA stabilește un cadru european comun în care încrederea în produsele digitale derivă din securitatea obligatorie, integrată încă din faza de concepție. Pe lângă armonizarea obligațiilor la nivelul statelor membre ale UE (unde este direct aplicabil), acest regulament ridică standardele la nivel global, influențând inclusiv practicile tuturor producătorilor din afara UE care doresc să aibă acces pe piața europeană.

2.3 Domeniul de aplicare (articolul 2 din CRA)

Conform articolului 2, CRA se aplică tuturor produselor cu elemente digitale a căror utilizare prevăzută sau utilizare previzibilă în mod rezonabil implică o conexiune de date directă sau indirectă, fizică sau logică, la un dispozitiv sau la o rețea.

2.3.1 Definiția produselor cu elemente digitale

Un produs cu elemente digitale (PDE) este orice produs software sau hardware, inclusiv soluții de prelucrare a datelor la distanță, care are componente digitale și este capabil de conectivitate.[4]

Domeniul de aplicare include, de asemenea, componentele hardware sau software ale PDE-urilor atunci când sunt introduse separat pe piață.

2.3.2 Excluderi

Anumite produse deja reglementate de legislația sectorială nu intră în domeniul de aplicare al CRA :

- Dispozitive medicale [Regulamentul (UE) 2017/745] și dispozitive pentru diagnostic in vitro [Regulamentul (UE) 2017/746].
- Autovehicule și sisteme conexe [Regulamentul (UE) 2019/2144].
- Echipamente pentru aviația civilă [Regulamentul (UE) 2018/1139].
- Echipamente maritime (Directiva 2014/90/UE).
- Piese de schimb identice pentru componente deja certificate.
- Produse dezvoltate exclusiv în scopuri de apărare sau de securitate națională.
- Produse special concepute pentru prelucrarea informațiilor clasificate.

[4] A se vedea articolul 3 alineatul (1) din Actul privind reziliența cibernetică (CRA).

2.4 Categoriile de produse din cadrul CRA

Conform CRA , produsele cu elemente digitale sunt clasificate în trei categorii principale, concepute pentru a adapta cerințele de conformitate în funcție de nivelul de risc:[5]

- **Produse implicite** – Această categorie cuprinde marea majoritate (aproximativ 90 %) a produselor cu elemente digitale. Aceste produse nu se încadrează în categoriile cu risc mai ridicat și își pot demonstra conformitatea prin autoevaluare.
- **Produse importante** (anexa III la CRA) – Acestea sunt produse cu risc mai ridicat și sunt împărțite în continuare în:
    - Clasa I: Necesită verificări mai stricte, deși adesea acestea se realizează tot prin autoevaluare, dacă există standarde armonizate sau specificații comune.
    - Clasa II: Reprezintă produsele mai critice și impun o evaluare a conformității realizatp de un terț.
- **Produse critice** (anexa IV la CRA) - Acestea prezintă cel mai mare risc de securitate cibernetică și trebuie să fie supuse certificării conform criteriilor comune europene (EUCC) de către un organism calificat de evaluare a conformității.

Categorie	Clasă	Semnificație succintă	Procedura de conformitate	Exemplu de produse
Produse implicite	–	PDE cu risc scăzut (~90% din total), dispozitive de larg consum sau de birou	Conformitatea este demonstrată prin control intern efectuat de producător, care conduce la emiterea unei declarații UE de conformitate.	Imprimante standard, unități USB, instrumente de productivitate de birou, difuzoare inteligente, becuri conectate, trackere de fitness
Produse importante	Clasa I	Produse cu risc mai ridicat, care necesită verificări mai stricte, deși adesea pot fi în continuare supuse autoevaluării dacă există standarde aplicabile.	Pentru produsele din clasa I, producătorii se pot baza pe evaluarea internă, cu condiția respectării standardelor armonizate sau a specificațiilor comune.	Termostate inteligente, camere web conectate, prelungitoare Wi-Fi pentru locuințe, încuietori inteligente, sonerii video, electrocasnice conectate (de exemplu, frigidere inteligente)
	Clasa II	Produse mai critice, necesită evaluare de către un terț	Produsele din Clasa II, prin contrast, necesită de obicei intervenția unui organism notificat pentru evaluare	Dispozitive medicale conectate (care nu sunt reglementate de MDR), sisteme de control industrial, gateway-uri IoT, sisteme de

[5] Pentru mai multe informații și clarificări detaliate, vă rugăm să consultați capitolul 5 din CRA101: Înțelegerea obligațiilor CRA; și capitolele 3 și 5 din Cadrul de evaluare metodologică a conformității al CRA.

			realizată de o terță parte.	control al accesului în clădiri, terminale de plată, sisteme de supraveghere conectate la cloud.
Produse critice	–	Cel mai mare risc de securitate cibernetică ar putea afecta grav siguranța, securitatea sau viața privată	Acestea trebuie să fie supuse certificării conform criteriilor europene comune (EUCC), un proces riguros care implică un organism acreditat de evaluare a conformității.	Echipamente de bază pentru rețele de telecomunicații, infrastructură 5G, module de securitate hardware (HSM), sisteme de gestionare a infrastructurilor critice, platforme de apărare în materie de securitate cibernetică bazate pe inteligență artificială.

2.5 Operatorii economici care intră în domeniul de aplicare al CRA

CRA stabilește o distribuție clară a obligațiilor de-a lungul lanțului de aprovizionare, asigurând faptul că securitatea cibernetică este abordată nu doar în etapa de fabricație, ci și în timpul importului, distribuției și modificării produselor.

Acest lanț de responsabilitate asigură faptul că securitatea cibernetică nu este tratată ca o cerință punctuală, ci ca o obligație continuă care revine fiecărui actor implicat în ciclul de viață al produsului.

Tabelul de mai jos prezintă exemple specifice pentru fiecare operator, evidențiind posibilele implicații legate de CRA .

Operatorul	Articolul CRA	Exemple de responsabilități	Exemple de scenarii ipotetice[6]
Producător	Articolul 13	• Proiectează produse în condiții de securitate (*secure by design / secure by default)* • Efectuează evaluări ale riscurilor • Elaborează și păstrează documentația tehnică • Aplică marcajul CE • Furnizează actualizări de securitate și gestionează vulnerabilitățile • Notifică vulnerabilitățile exploatate și incidentele în termen de 24 de ore	*Un producător de termostate inteligente descoperă o vulnerabilitate. Acesta trebuie să lanseze o actualizare de firmware, să informeze clienții și să raporteze incidentul autorităților în termen de 24 de ore.*

[6] **DECLARAȚIE:** În absența unor dispoziții legislative detaliate privind transpunerea CRA , exemplele prezentate mai jos reprezintă scenarii fictive, dar realiste, bazate pe o interpretare provizorie a regulamentului. Produsele, contextele și scenariile menționate pot, în cele din urmă, să nu intre în domeniul de aplicare al CRA sau să constituie doar reprezentări parțial exacte, în special în urma transpunerii formale a CRA .

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Importator[7]	Articolul 19	• Introducerea produselor pe piața UE numai dacă sunt conforme • Verificarea marcajului CE și a conformității • Păstrarea dosarelor tehnice timp de 10 ani • Cooperarea cu autoritățile	*Un importator de firewall-uri de rețea trebuie să asigure marcajul CE și conformitatea înainte de vânzare. Dacă rebranduiește produsul sau îi modifică software-ul, este considerat producător în temeiul CRA.*
Distribuitor[8]	Articolul 20	• Confirmarea marcajului CE și a conformității înainte de distribuire • Evitarea distribuirii de produse riscante • Notificarea autorităților cu privire la vulnerabilități/incidente	*Un distribuitor de sonerii video conectate detectează o vulnerabilitate care expune datele de autentificare. Acesta trebuie să oprească vânzările, să notifice autoritățile și să se coordoneze cu producătorul. Dacă comercializează produsul sub propria marcă, este considerat producător.*
Administratori de software open-source	Articolul 24	• Asigurarea că software-ul este întreținut în siguranță • Furnizarea de informații privind vulnerabilitățile • Cooperarea cu autoritățile și părțile interesate	*Un mentenant open-source găsește o vulnerabilitate într-o bibliotecă utilizată în dispozitivele IoT. Acesta publică corecțiile și se coordonează cu utilizatorii pentru a atenua problema.*

2.5.1 Reprezentant autorizat (RA) – articolul 18

(Nu reprezintă o categorie de operatori independenți în același sens ca producătorii, importatorii sau distribuitorii ci, mai degrabă, o entitate desemnată de un producător din afara UE.)

- Acționează ca punct de contact al UE pentru producătorii din afara UE.
- Deține documentația tehnică și declarația de conformitate UE.
- Răspunde la solicitările de informații din partea autorităților.
- Cooperează cu autoritățile și poate transmite notificări dacă este delegat.

Exemplu: Un reprezentant autorizat (RA) cu sediul în UE pentru un producător de senzori IoT din afara UE furnizează documentație tehnică completă în timpul unui audit sau răspunde la întrebări privind actualizările de securitate și gestionarea vulnerabilităților.

2.5.2 Modificări substanțiale – articolul 22

Orice operator (inclusiv importatori, distribuitori sau părți terțe) care modifică în mod substanțial un produs cu elemente digitale într-un mod care afectează conformitatea este considerat producător din punct de vedere juridic și trebuie să respecte toate obligațiile care revin producătorului (documentație, marcaj CE, gestionarea vulnerabilităților, raportarea incidentelor). Aceasta nu reprezintă o categorie distinctă de operatori, ci o reclasificare juridică.

[7] Articolul 22: Importatorii devin producători dacă introduc pe piață produse sub nume/marcă proprie sau le modifică în mod substanțial.

[8] Articolul 22: Distribuitorii devin producători dacă plasează produsele sub nume/marcă proprie sau le modifică în mod substanțial.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

2.6 Exemple de scenarii ipotetice legate de produs[9]

Următoarele sunt exemple de implicații posibile ale aplicării CRA. Acestea sunt scenarii condiționate, care ilustrează ce s-ar putea întâmpla, mai degrabă decât cerințe propriu-zise. Fiecare exemplu evidențiază aspecte operaționale, de reglementare și legate de lanțul de aprovizionare.

Vulnerabilitatea dispozitivelor smart home *Un termostat inteligent comercializat pe scară largă ar putea fi descoperit că permite accesul neautorizat de la distanță la rețeaua casnică. Producătorii ar putea fi nevoiți să emită o actualizare urgentă a firmware-ului, să se coordoneze cu distribuitorii pentru a opri transporturile de unități afectate și să notifice autoritățile. Utilizatorii finali s-ar putea confrunta cu întreruperi temporare ale serviciilor. Acest scenariu arată modul în care obligațiile CRA pot declanșa coordonarea între actori și răspunsuri operaționale.*	**Incident cu cameră de securitate conectată** *O cameră de securitate de interior conectată în rețea ar putea fi descoperită că transmite fluxuri video necriptate către servere terțe. Distribuitorii ar putea fi nevoiți să oprească vânzările, importatorii ar putea fi nevoiți să revizuiască documentația tehnică, iar producătorii ar putea lansa o corecție pentru a cripta datele. Autoritățile ar putea solicita raportarea vulnerabilității, ilustrând impactul CRA confidențialității consumatorilor și a obligațiilor de securitate cibernetică.*
Defecienţă la un gateway IoT industrial *Un gateway IoT utilizat în clădiri inteligente ar putea fi descoperit că permite accesul neautorizat la senzorii conectați. Producătorii ar putea fi nevoiți să lanseze o actualizare software, distribuitorii ar putea opri livrările lotului afectat, iar importatorii ar putea fi solicitați să verifice dosarele de conformitate actualizate. Operatorii clădirilor ar putea fi nevoiți să aplice corecțiile, arătând impactul CRA asupra IoT-ului industrial și a continuității operaționale.*	**Exploatarea unei imprimantei de birou conectate** *O imprimantă multifuncțională de rețea multifuncțională ar putea fi descoperită ca având un defect care permite atacatorilor să acceseze rețeaua de birou prin intermediul dispozitivului. Producătorul ar putea lansa o actualizare de firmware, în timp ce distribuitorii se asigură că unitățile afectate sunt reținute de la vânzare până la aplicarea corecției. Importatorii ar putea fi responsabili de verificarea conformității cu CE a noilor livrări. Acest exemplu ilustrează rolul CRA în asigurarea securității cibernetice chiar și pentru dispozitivele de birou cu risc scăzut.*
Vulnerabilitate la un bec inteligent *O marcă de becuri conectate ar putea fi descoperită că este susceptibilă la preluare de la distanță, putând deveni parte a unei rețele botnet. Producătorii ar putea furniza o actualizare de securitate over-the-air, distribuitorii ar putea notifica comercianții să oprească vânzarea unităților vulnerabile, iar importatorii ar putea fi nevoiți să păstreze documentația tehnică pentru audit. Utilizatorii finali ar fi îndrumați să aplice actualizările, arătând implicațiile CRA pentru siguranța IoT-ului de consum*	**Breșă la o sonerie video conectată la cloud** *O sonerie video conectată la cloud ar putea ar putea expune datele de autentificare din cauza unui design API nesecurizat. Producătorul ar putea actualiza firmware și metodele de autentificare în cloud, în timp ce importatorii și distribuitorii coordonează documentația de conformitate și comunicarea către utilizatori. Autoritățile ar putea fi notificate în cazul în care vulnerabilitatea este exploatată în mod activ. Acest scenariu evidențiază influența CRA asupra programelor informatice, a firmware-ului și a supravegherii ulterioare introducerii pe piață.*

[9] **DECLARAȚIE:** a se vedea nota nr. 6

2.7 De la domeniul de aplicare al CRA la cerințele legate de CRA ale proiectului SECURE

Chiar dacă legislația CRA va deveni pe deplin aplicabilă abia în decembrie 2027, societăţile sunt puternic încurajate să înceapă încă de pe acum alinierea proceselor lor la cerințele CRA. Anticiparea obligațiilor nu numai că va facilita tranziția odată ce regulamentul va deveni pe deplin aplicabil, dar va consolida și nivelul de pregătire pentru piață și reziliența solicitanților pe termen scurt.

Scopul principal al proiectului SECURE este de a sprijini IMM-urile în pregătirea pentru conformitatea cu CRA prin finanțarea unor activități și servicii care contribuie direct la îndeplinirea obligațiilor CRA. Verificarea relevanței CRA va face parte din procesul de evaluare efectuat de partenerii SECURE desemnați. Solicitanții trebuie să demonstreze că activitățile propuse sunt clar legate de obligațiile CRA și că se încadrează în domeniul de aplicare al regulamentului.

3 Activități, servicii și bunuri finanțabile aferente CRA în cadrul Apelului Deschis

Următoarea listă oferă exemple generale de activități, bunuri și servicii finanțabile, menite să servească drept ghid pentru solicitanți în identificarea tipurilor de activități eligibile pentru a primi sprijin. Cu toate acestea, pe lângă aceste exemple, pot fi propuse și servicii suplimentare dacă acestea contribuie în mod demonstrabil și direct la realizarea conformității CRA.

Notă pentru solicitanți:

Pentru inspirație suplimentară cu privire la activitățile finanțabile, solicitanții sunt încurajați să consulte orientările specifice publicate pe canalele web SECURE, inclusiv Înțelegerea obligațiilor CRA – CRA 101, Cadrul metodologic de evaluare a conformității al CRA și cerințele esențiale de securitate cibernetică ale CRA (Anexa I, Partea I). Acestea oferă modele, recomandări și sugestii privind conformitatea cu CRA pe lângă exemplele enumerate mai jos.

3.1 Categoria 1: Audit realizat de un organism terț acreditat, cu emiterea certificatului CRA

NOTĂ IMPORTANTĂ: Această activitate nu va fi eligibilă pentru finanțare în primul apel. Va deveni eligibilă abia după transpunerea CRA în statele membre ale Uniunii și după identificarea mecanismelor și standardelor pentru certificarea produselor.

Un audit efectuat de o terță parte acreditată de încredere este o evaluare formală și independentă a conformității, realizată de o organizație acreditată în cadrul aplicabil al UE. Scopul acestuia este de a verifica dacă produsul îndeplinește cerințele esențiale de securitate cibernetică prevăzute în Actul privind Reziliența Cibernetică (CRA), inclusiv principiile de securitate prin proiectare (security by design), procesele de gestionare a vulnerabilităților și mecanismele de actualizare sigure. Acest serviciu include un plan de audit structurat, o analiză aprofundată a documentației, testare funcțională și de securitate, identificarea neconformităților cu acțiuni corective și, după remedierea cu succes a acestora, emiterea unui certificat conform CRA. O astfel de certificare este o demonstrație concretă a conformității, esențială atât pentru accesul pe piață, cât și pentru încrederea clienților.

3.2 Categoria 2: CRA – Evaluarea securității cibernetice, gestionarea riscurilor și evaluarea conformității CRA – Modulul 1: Analiza decalajelor de conformitate cu CRA

Această analiză a decalajelor de conformitate cu CRA examinează în mod sistematic dacă procesele-suport aferente fabricării sau distribuirii unui produs care intră sub incidența CRA îndeplinesc cerințele prevăzute de regulament. Ea compară practicile curente cu controalele impuse, precum divulgarea vulnerabilităților, jurnalizarea, actualizările de securitate și documentația, și identifică eventualele deficiențe. Rezultatul constă într-un registru al neconformităților prioritizat, care îi permite solicitantului să înțeleagă clar măsurile tehnice și organizatorice specifice necesare pentru atingerea conformității depline.

Exemple de rezultate preconizate	Descriere	Exemple de indicatori-cheie de performanță
Raport de analiză a decalajelor de conformitate cu CRA	*Document care evidențiază decalajele dintre procesele actuale și cerințele prevăzute de CRA.*	*Numărul controalelor CRA evaluate*
Registrul de analiză a decalajelor	*Tabel sau foaie de calcul care enumeră deficiențele identificate și nivelurile de criticitate.*	*Procentul decalajelor identificate documentate în registrul decalajelor*
Lista de verificare a conformității	*Document care atestă respectarea controalelor-cheie prevăzute de CRA: divulgarea vulnerabilităților, jurnalizarea, actualizările și documentația.*	*Numărul de decalaje cu prioritate ridicată identificate în raport cu decalajele totale*
Rezumatul constatărilor	*Prezentare sau PDF care sintetizează principalele decalaje și acțiunile recomandate.*	*Rata de finalizare a listei de verificare a conformității*
Pachet de documente justificative	*Dosar cu documente justificative care demonstrează practicile actuale și decalajele identificate (politici sau proceduri rezultate).*	*Nr. de politici elaborate*

Exemplu de jaloane (milestones):

- Finalizarea evaluării inițiale a controalelor CRA și identificarea decalajelor
- Predarea registrului prioritar al decalajelor și a listei de verificare a conformității
- Transmiterea raportului final de analiză a decalajelor de conformitate cu CRA împreună cu un rezumat executiv

3.3 Categoria 3: Guvernanța securității cibernetice, gestionarea riscurilor și evaluarea conformității CRA - Modulul 2: Analiza nevoilor de conformitate cu CRA și a riscurilor

Această evaluare analizează nevoile de conformitate în raport cu riscurile identificate de-a lungul întregului ciclu de viață al produsului. Acesta ia în considerare scenariile de amenințare, analiza probabilității și a impactului, dependența de componente furnizate de terți, precum și posibila expunere la riscuri de reglementare. Riscurile sunt corelate cu controalele relevante prevăzute de CRA , asigurând astfel alinierea strategiilor de diminuare a riscurilor atât la cerințele legale, cât și la cele de securitate.

Exemple de livrabile	Descriere	Exemple de indicatori-cheie de performanță (KPI)
Raport de evaluare a riscurilor în raport cu CRA	*Document care corelează riscurile identificate cu controalele prevăzute de CRA / modele de analiză a riscurilor*	*Numărul riscurilor identificate și clasificate (scăzut/mediu/ridicat))*
Document de analiză a scenariului de amenințare	*Raport care detaliază amenințările potențiale, probabilitatea și impactul acestora*	*Numărul de amenințări analizate și de impacturi cuantificate*

Registrul riscurilor aferente componentelor furnizate de terți	*Foaie de calcul care enumeră dependențele și riscurile asociate*	*Numărul de componente critice furnizate de terți evaluate*
Evaluarea expunerii la riscuri de reglementare	*Document care sintetizează sancțiunile și obligațiile potențiale în caz de neconformitate (NC)*	*Numărul de NC / regulamentări / controale analizate*
Pachet de recomandări pentru diminuarea riscurilor	*Prezentare sau PDF care descrie acțiunile corective sugerate și prioritățile*	*Numărul de măsuri de diminuare a riscurilor propuse*

Exemplu de jaloane (milestones):

- Finalizarea cartografierii scenariilor de amenințare și identificarea inițială a riscurilor
- Livrarea registrului de riscuri și evaluarea expunerii la riscuri de reglementare
- Transmiterea Raportului final privind necesitățile de conformitate și analiza riscurilor CRA

3.4 Categoria 2: Guvernanța securității cibernetice, gestionarea riscurilor și evaluarea conformității CRA - Modulul 3: Planul de remediere pentru conformitatea cu CRA

Planul de remediere pentru conformitatea cu CRA reprezintă o foaie de parcurs structurată și aplicabilă pentru remedierea lacunelor de conformitate identificate Acesta definește activitățile de remediere, atribuie responsabilități, stabilește termene și detaliază resursele necesare. Planul este aliniat cu ciclurile de dezvoltare ale organizației, asigurând integrarea îmbunătățirilor de conformitate în lansările regulate de produs, și nu tratarea lor ca intervenții punctuale

Exemple de rezultate preconizate	Descriere	Exemple de indicatori-cheie de performanță
Document plan de remediere al CRA	*Foaie de parcurs realizabilă care detaliază activitățile, responsabilitățile și termenele de remediere*	*Procentul de lacune identificate cu acțiuni de remediere atribuite*
Plan de alocare a resurselor	*Foaie de calcul sau diagramă care indică personalu alocat, bugetul și instrumentele pentru fiecare sarcină de remediere*	*Numărul de sarcini de remediere finalizate conform programului*
Instrument de urmărire a activității de remediere	*Jurnal sau tablou de bord care prezintă progresele înregistrate în ceea ce privește acțiunile corective*	*Numărul de resurse alocate în raport cu cele planificate*
Registru actualizat de închidere a decalajelor	*Document care prezintă situația lacunelor identificate anterior*	*Reducerea în timp a numărului de neconformități critice*
Dovezi privind măsurile de remediere puse în aplicare	*Documente tehnice sau materiale care demonstrează că s-a realizat punerea în aplicare a unei măsuri de remediere*	*Nr. de dovezi încărcate care evaluează punerea în aplicare a măsurilor de remediere*

Exemplu de jaloane (milestones):

- Aprobarea planului inițial de remediere de către părțile interesate ale proiectului
- Finalizarea a x % din activitățile de remediere
- Remedierea completă a decalajelor de conformitate identificate și finalizarea Planului de remediere

3.5 Categoria 3: Formare privind cerințele CRA

Un program de formare direcționat, care oferă personalului o înțelegere clară a obligațiilor prevăzute de CRA și a cerințelor esențiale de securitate cibernetică. Temele abordate includ principiile de proiectare sigură, obligațiile privind documentația, căile de evaluare a conformității, obligațiile de supraveghere post-introducere pe piață și gestionarea vulnerabilităților. Scopul este de a crea un nivel comun de înțelegere în toate echipele relevante, reducând la minimum erorile și asigurând o abordare unitară a conformității.

Exemple de rezultate preconizate	Descriere	Exemple de indicatori-cheie de performanță
Document programă de formare	*Programa detaliată care acoperă obligațiile CRA și cerințele în materie de securitate cibernetică*	*Numărul de cerințe acoperite*
Diapozitive prezentare de formare	*PowerPoint sau PDF pentru sesiuni de formare*	*Numărul de documente distribuite participanților*
Înregistrări de prezență și de finalizare	*Lista membrilor personalului care au participat și au finalizat formarea / Înregistrarea sesiunii de formare*	*Numărul de membri ai personalului formați* *Numărul de sesiuni de formare desfășurate*
Rezultatele evaluării formării	*Rezultatele chestionarelor sau testelor pentru măsurarea înțelegerii*	*Procentul de participanți care au promovat evaluarea formării /* *Scorul mediu al participanților la evaluările formării*
Raport de feedback privind formarea	*Rezumatul feedbackului și al sugestiilor de îmbunătățire ale participanților*	*Ratingul de satisfacție al participanților*

Exemplu de jaloane (milestones):

- Finalizarea sesiunii inițiale de formare pentru toate echipele relevante
- 100 % din personal promovează evaluarea aferentă formării
- Întocmirea Raportului final de formare și centralizarea feedback-ului

3.6 Categoria 4: Cursuri de formare în materie de securitate cibernetică legate de CRA

Perfecționare practică și tehnică pentru dezvoltatori, ingineri și personalul de securitate, în vederea alinierii activităților curente la cerințele prevăzute de CRA. Temele pot include practici de programare securizată, tehnici de modelare a amenințărilor, gestionarea în condiții de securitate a componentelor open-source și

remedierea vulnerabilităților identificate în cadrul evaluărilor. Instruirea este concepută astfel încât să aibă un impact operațional imediat.

Pentru un exemplu de livrabil, consultați secțiunea „Activitate de instruire privind cerințele CRA".

3.7 Categoria 5: Sprijin de specialitate în implementarea proiectului de conformitate CRA

Asistență de specialitate, sub formă de consultanță și sprijin practic în implementarea proiectului, pentru coordonarea procesului de conformitate cu CRA. Experții oferă îndrumare tehnică, revizuiesc documentele și materialele elaborate, coordonează fluxurile de lucru aferente remedierii și monitorizează progresul. Această activitate este deosebit de valoroasă pentru IMM-urile care nu dispun de expertiză internă în materie de CRA, asigurând acuratețe și eficiență pe tot parcursul proiectului.

Exemple de rezultate preconizate	Descriere	Exemple de indicatori-cheie de performanță
Rapoarte de îndrumare tehnică	*Documentația privind consilierea oferită cu privire la măsurile de conformitate*	*Numărul de măsuri de conformitate acoperite*
Artefacte revizuite	*Politici, proceduri sau documente tehnice actualizate*	*Numărul de politici elaborate și/sau puse în aplicare*
Jurnale de coordonare a fluxului de lucru	*Evidențe ale sarcinilor, atribuirilor și progresului*	*Procentul de artefacte ale proiectului examinate și aprobate*
Rapoarte de monitorizare a progreselor	*Monitorizarea etepelor cheie de conformitate și remedierea lacunelor*	*Numărul de lacune de conformitate abordate pe baza îndrumărilor experților*
Rezumatele sesiunilor de consultanţă	*Notele de ședință care detaliază recomandările și etapele următoare*	*Numărul de reuniuni* *Numărul de recomandări puse în aplicare*

Exemplu de jaloane (milestones):

- Finalizarea analizei inițiale a conformității de către experți
- Finalizarea planurilor de remediere a fluxului de lucru
- Transmiterea raportului consolidat de monitorizare a progreselor înregistrate

3.8 Categoria 6: Teste de vulnerabilitate

Evaluări periodice ale vulnerabilităților produsului, care acoperă componentele software, firmware și hardware pentru identificarea punctelor slabe exploatabile. Evaluările pot include analize statice și dinamice, revizuiri de configurație și verificări ale dependențelor. Detectarea timpurie a vulnerabilităților este esențială pentru remedierea acestora înainte ca ele să poată fi exploatate, contribuind în mod direct la conformitatea cu CRA.

Exemple de rezultate preconizate	Descriere	Exemple de indicatori-cheie de performanță
Rapoarte de evaluare a vulnerabilităților și plan de remediere	*Documentarea detaliată a vulnerabilităților detectate și a remedierilor sugerate*	*Numărul de vulnerabilități identificate* *Numărul de VA efectuate* *Numărul de sisteme/aplicații analizate* *Procentul de acoperire al sistemelor/componentelor testate*
Jurnale de analiză statică și dinamică	*Înregistrări de la scanări automate de cod și teste de rulare*	
Rapoarte de revizuire a configurației	*Evaluarea configurațiilor sistemelor și dispozitivelor*	*Distribuția gravității vulnerabilităților detectate*
Rapoarte de verificare a dependențelor	*Analiza bibliotecilor sau componentelor terțe*	*Numărul de biblioteci testate*
Patch-uri și corecții	*Implementarea corecțiilor și remedierilor pentru vulnerabilitățile identificate*	*Numărul de vulnerabilități remediate*

Exemplu de jaloane (milestones):

- Finalizarea evaluării inițiale a vulnerabilităților
- Implementarea acțiunilor de remediere a vulnerabilităților critice
- Aprobarea raportului final de evaluare a vulnerabilității de către echipa de conformitate

3.9 Categoria 7: Teste de laborator

Testare controlată, realizată în laborator, pentru a verifica dacă funcțiile de securitate ale unui produs, precum criptarea, autentificarea și controlul accesului, funcționează conform intenției, în condiții reproductibile. Aceste teste furnizează dovezi solide că produsul îndeplinește cerințele esențiale prevăzute de CRA.

Exemple de rezultate preconizate	Descriere	Exemple de indicatori-cheie de performanță
Rapoarte de evaluare a vulnerabilităților și plan de remediere	*Documentarea detaliată a vulnerabilităților detectate și a remedierilor sugerate*	*Numărul de vulnerabilități identificate* *Numărul de VA efectuate* *Numărul de sisteme/aplicații analizate* *Procentul de acoperire al sistemelor/componentelor testate*
Jurnale de analiză statică și dinamică	*Înregistrări de la scanări automate de cod și teste de rulare*	
Rapoarte de revizuire a configurației	*Evaluarea configurațiilor sistemelor și dispozitivelor*	*Distribuția gravității vulnerabilităților detectate*
Rapoarte de verificare a dependențelor	*Analiza bibliotecilor sau componentelor terțe*	*Numărul de biblioteci testate*
Patch-uri și corecții	*Implementarea corecțiilor și remedierilor pentru vulnerabilitățile identificate*	*Numărul de vulnerabilități remediate*

Exemplu de jaloane (milestones):

- Finalizarea testelor inițiale de laborator pentru toate elementele de securitate vizate
- Verificarea funcționalității mecanismelor de criptare, autentificare și control al accesului
- Revizuirea și aprobarea orientărilor tehnice și a materialelor rezultate de către părțile interesate

3.10 Categoria 8: Teste de penetrare

Atacuri cibernetice simulate, autorizate, realizate de testeri cu experiență pentru a evalua gradul real de exploatabilitate al vulnerabilităților. În contextul CRA, testarea de penetrare acoperă multiple suprafețe de atac,firmware, API-uri, interfețe cloud, sisteme încorporate și demonstrează atât conformitatea, cât și reziliența produsului.

Exemple de rezultate preconizate	Descriere	Exemple de indicatori-cheie de performanță
Raport de teste de penetrare și plan de remediere	*Exploatări documentate și remedieri sugerate*	*Numărul de exploatări reușite* *Sisteme testate* *Acoperirea suprafeței de atac*
Exploatări de tip Proof-of-Concept	*Demonstrații de atacuri*	*Numărul de puncte de contact(POC-uri)* *Gravitatea vulnerabilităților*
Verificarea configurației și a dependențelor	*Evaluarea riscurilor de sistem și ale terților*	*Numărul de configurări greșite* *Biblioteci/componente testate*
Verificarea remedierii	*Validarea remedierilor*	*Numărul de vulnerabilități atenuate*

Exemplu de jaloane (milestones):

- Finalizarea testului inițial de penetrare
- Demonstrarea exploatărilor critice
- Măsuri de atenuare aplicate și verificate

3.11 Categoria 9: Serviciu de evaluare de către terți pentru CRA

NOTĂ IMPORTANTĂ: Această activitate nu va fi eligibilă pentru finanțare în cadrul primului apel, ci va deveni eligibilă după transpunerea CRA în legislațiile fiecărui stat membru al Uniunii Europene și după identificarea mecanismelor și standardelor pentru certificarea produselor.

O evaluare independentă realizată de o organizație autorizată, în scopul verificării conformității cu CRA. Acest serviciu oferă o verificare imparțială a conformității și este deosebit de important pentru categoriile de produse cu risc ridicat, pentru care evaluarea de către o terță parte este impusă de CRA.

3.12 Categoria 10: Instrumentul de autoevaluare al CRA

Un instrument structurat de autoevaluare, cum ar fi o listă de verificare sau o platformă software care ghidează organizațiile prin cerințele prevăzute de CRA. Acesta facilitează identificarea timpurie a decalajelor de conformitate, sprijinind remedierea proactivă și reducând dependența de măsuri reactive.

Exemple de rezultate preconizate	Descriere	Exemple de indicatori-cheie de performanță
Rapoarte de autoevaluare	*Evaluări finalizate care indică starea de conformitate*	*Numărul de evaluări finalizate* *Lacune de conformitate identificate* *Acoperirea cerințelor CRA*
Rezultate ale listei de verificare	*Îndrumare structurată și verificări automatizate*	*Numărul de elemente evaluate* *Procentul de cerințe evaluate*
Planul de remediere	*Acțiuni pentru abordarea decalajelor detectate*	*Numărul de decalaje abordate* *Timpul necesar pentru punerea în aplicare a acțiunilor corective*
Tabloul de bord privind urmărirea progreselor	*Vizualizarea îmbunătățirilor aduse conformității*	*Rata de îmbunătățire în timp* *Numărul de probleme închise*

Exemplu de jaloane (milestones):

- Finalizarea autoevaluării inițiale
- Identificarea decalajelor de conformitate
- Implementarea acțiunilor de remediere

3.13 Categoria 11: Dezvoltare software – Securitate din faza de proiectare (Security by design) pentru produsele CRA

Integrarea securității în ciclul de viață al dezvoltării software (SDLC), în conformitate cu principiile CRA. Aceasta include modelarea amenințărilor, standarde de programare securizată, gestionarea Software Bill of Materials (SBOM) și testarea de securitate integrată în fluxurile CI/CD.

Exemple de rezultate preconizate	Descriere	Exemple de indicatori-cheie de performanță
Proiectare securizată și modele de amenințări	*Documentarea cerințelor de securitate și a scenariilor de amenințare*	*Numărul de amenințări identificate* *Acoperirea componentelor critice*
Codul securizat și SBOM	*Cod dezvoltat în conformitate cu standardele de codificare securizate și SBOM menținut*	*Numărul de probleme de cod detectate* *Procentul componentelor cu SBOM*
Rapoarte de testare a securității	*Rezultatele testelor statice, dinamice și de dependență integrate în ci/cd*	*Numărul de vulnerabilități detectate* *Procentul de acoperire a testului*
Remediere și Verificare	*Remedieri aplicate și verificate în conducta de dezvoltare*	*Numărul de probleme soluționate* *Timpul până la remediere*

Exemplu de jaloane (milestones):

- Finalizarea modelării amenințărilor
- Integrarea practicilor de programare securizată și SBOM
- Efectuarea de testelor automate de securitate

3.14 Categoria 12: Continuitatea activității, planificarea incidentelor și a răspunsului la incidente pentru produsele și procesele vizate de CRA

Dezvoltarea unor cadre operaționale pentru detectarea, răspunsul la incidente și recuperarea în urma acestora, care să respecte cerințele prevăzute de CRA. Aceasta include proceduri de mentenanță urgentă, implementarea actualizărilor securizate și protocoale de comunicare cu clienții în cazul producerii unor incidente.

Exemple de rezultate preconizate	Descriere	Exemple de indicatori-cheie de performanță
Planul de răspuns la incidente	*Proceduri documentate pentru detectarea incidentelor, răspunsul la acestea și redresarea în urma acestora*	*Numărul de incidente detectate* *Timpul mediu de răspuns (MTTR)* *Acoperirea proceselor critice*
Planul de continuitate a afacerii	*Cadrul pentru menținerea operațiunilor esențiale în timpul perturbărilor*	*Obiectivele privind timpul de recuperare (RTO)* *Obiectivele punctului de recuperare (RPO)* *Procentajul de integralitate a planului*
Teste și Rapoarte de simulare	*Rezultatele exercițiilor, simulărilor și exercițiilor de scenarii*	*Numărul de încercări efectuate* *Eficacitatea răspunsului* *Rata de închidere a decalajelor*
Protocoale de comunicare	*Proceduri definite pentru notificarea părților interesate și a clienților în timpul incidentelor*	*Numărul de comunicări executate la timp* *Satisfacția părților interesate*

Exemplu de jaloane (milestones):

- Finalizarea planurilor inițiale de incident și de continuitate a activității
- Executarea primei simulări/exercițiu
- Implementarea acțiunilor corective rezultate în urma testelor

3.15 Categoria 13: Evaluarea riscurilor și a securității lanțului de aprovizionare

Evaluare cuprinzătoare a furnizorilor terți și a componentelor acestora, pentru a asigura respectarea cerințelor de securitate prevăzute de CRA. Activitățile includ audituri ale furnizorilor, clauze contractuale privind securitatea și evaluarea riscurilor bazată pe SBOM, în vederea reducerii vulnerabilităților din lanțul de aprovizionare.

Exemple de rezultate preconizate	Descriere	Exemple de indicatori-cheie de performanță
Rapoarte de evaluare a securității furnizorilor	*Evaluarea furnizorilor terți în raport cu cerințele CRA*	*Numărul de furnizori evaluați* *Gravitatea riscurilor identificate* *Acoperirea furnizorilor critici*
Audit și Rapoarte de verificare	*Dovezi provenite din auditurile la fața locului sau de la distanță ale furnizorilor*	*Numărul de audituri efectuate* *Deficiențe de conformitate detectate*
Analiza riscurilor bazată pe SBOM	*Evaluarea componentelor de la terți utilizând lista de materiale software*	*Numărul de componente analizate* *Vulnerabilitățile identificate*
Remediere și Plan de atenuare	*Acțiuni de abordare a riscurilor din lanțul de aprovizionare*	*Numărul de riscuri atenuate* *Timpul necesar pentru punerea în aplicare a acțiunilor corective*

Exemplu de jaloane (milestones):

- Finalizarea evaluărilor inițiale ale furnizorilor
- Executarea auditurilor furnizorilor
- Identificarea și atenuarea riscurilor critice din lanțul de aprovizionare

3.16 Categoria 14: Conformitate privind Protecția datelor și confidențialitatea

Alinierea proiectării și funcționării produsului la legislația privind protecția datelor, inclusiv GDPR, în concordanță cu obligațiile prevăzute de CRA. Aceasta asigură abordarea integrată a securității și confidențialității, acoperind minimizarea datelor, stocarea securizată și gestionarea încălcărilor de securitate.

Exemple de rezultate preconizate	Descriere	Exemple de indicatori-cheie de performanță
Evaluarea impactului asupra protecției datelor (DPIA)	*Evaluarea activităților de prelucrare a datelor în raport cu CRA și cu cerințele de confidențialitate*	*Numărul de DPIA finalizate* *Numărul de decalaje în materie de conformitate identificate*
Confidențialitate și Implementarea controalelor de securitate	*Integrarea minimizării datelor, a criptării și a controalelor de acces*	*Procentul de sisteme cu controale puse în aplicare* *Numărul de defecțiuni de control detectate*
Răspuns la încălcare și Plan de raportare	*Proceduri pentru detectarea, raportarea și atenuarea încălcărilor securității datelor*	*Timpul mediu de detectare/răspuns (MTTD/MTTR)* *Numărul de încălcări raportate la timp*
Rapoarte de verificare a conformității	*Documentarea auditurilor și a analizelor care confirmă respectarea vieții private*	*Numărul de audituri efectuate* *Numărul de probleme remediate*

Exemplu de jaloane (milestones):

- Finalizarea evaluării inițiale a impactului asupra protecției datelor (DPIA) inițiale
- Implementarea controalelor de confidențialitatea și securitatea
- Executarea exercițiilor de răspuns la breșele de securitate

3.17 Categoria 15: Sprijin privind obligațiile de reglementare și documentația aferentă CRA

NOTĂ IMPORTANTĂ: Această activitate nu va fi eligibilă pentru finanțare în timpul primului apel. Va deveni eligibilă abia după transpunerea CRA în fiecare stat membru al Uniunii și după identificarea mecanismelor și standardelor pentru certificarea produselor.

Sprijin pentru pregătirea și menținerea documentației tehnice și a evidențelor de reglementare impuse de CRA, cum ar fi declarațiile de conformitate, planurile de supraveghere post-introducere pe piață și politicile de divulgare a vulnerabilităților.

3.18 Categoria 16: Servicii și instrumente de monitorizare, protecție și prevenire

Implementarea unor instrumente și servicii pentru monitorizare continuă, prevenirea proactivă a amenințărilor și detectarea incidentelor. Exemplele includ sisteme de detecție a intruziunilor, scanare antimalware, controlul accesului, gestionarea privilegiilor și soluții de criptare.

Exemple de rezultate preconizate	Descriere	Exemple de indicatori-cheie de performanță
Monitorizare și Instrumente de detectare	Implementarea scanerelor malware IDS și a sistemelor de înregistrare	Numărul de sisteme monitorizate Numărul de amenințări detectate
Accessul și Managementul privilegiilor	Implementarea controalelor pentru gestionarea accesului și privilegiilor utilizatorilor	Numărul de conturi privilegiate gestionate Încălcări ale accesului detectate
Criptarea și Protecția datelor	Implementarea soluțiilor de criptare și stocare securizată	Procentul de date criptate Numărul de incidente legate de protecția datelor
Prevenirea amenințărilor și Rapoarte de răspuns	Rapoarte privind amenințările detectate, măsurile de prevenire și acțiunile de atenuare	Numărul de amenințări prevenite Timpul mediu de răspuns (MTTR)

Exemplu de jaloane (milestones):

- Implementarea instrumentelor de monitorizare și protecție
- Implementarea controalelor de acces și de gestionare a privilegiilor
- Executarea procedurilor de detectare și prevenire a amenințărilor

3.19 Bunuri și licențe

Solicitanții pot achiziționa, de asemenea, bunuri sau tehnologii atunci când astfel de achiziții sunt necesare pentru realizarea uneia dintre activitățile eligibile menționate mai sus sau atunci când acestea sunt esențiale pentru implementarea cu succes a proiectului ori pentru atingerea obiectivelor de conformitate cu CRA. În special, achizițiile eligibile pot include tehnologii de securitate cibernetică și reziliență digitală destinate protejării sistemelor informatice, mediilor de producție sau produselor propriu-zise.

Vă rugăm să rețineți că costurile aferente bunurilor și licențelor vor fi acoperite doar pentru perioada de utilizare din cadrul intervalului de 180 de zile aferent implementării proiectului. Exemplele pot include, fără a se limita la acestea:

- instrumente de securitate a rețelei, precum firewall-uri, sisteme de detectare și prevenire a intruziunilor (IDS/IPS) și gateway-uri de generație nouă;
- tehnologii de protecție a datelor, inclusiv software de criptare, sisteme sigure de gestionare a cheilor și soluții de prevenire a pierderii datelor (DLP);
- soluții de securitate pentru endpoint-uri și dispozitive, precum antivirus, soluții de detectare și răspuns la nivel de endpoint (EDR), Extended Detection and Response (XDR) sau soluții de management al dispozitivelor mobile (MDM);
- instrumente de gestionare a vulnerabilităților și a conformității, inclusiv software pentru teste de penetrare, sisteme automate de gestionare a patch-urilor și scanere de vulnerabilități;
- medii securizate pentru dezvoltare și monitorizare, precum platforme de analiză a codului, instrumente de monitorizare continuă a securității și sisteme de jurnalizare / alertare (de exemplu, SIEM);
- soluții pentru protecția mediului de producție, de exemplu firewall-uri industriale, sisteme de detectare a intruziunilor pentru tehnologie operațională (OT) și dispozitive de control al accesului;
- servicii cloud securizate și instrumente de securitate pentru containere, inclusiv platforme de protecție a sarcinilor de lucru în cloud (CWPP) și soluții de scanare a containerelor;
- soluții de gestionare a identității și accesului (IAM), sisteme de autentificare multifactor (MFA) și instrumente de gestionare a accesului privilegiat (PAM).
- instrumente de gestionare a Software Bill of Materials (SBOM) și soluții de scanare a dependențelor, pentru securitatea lanțului de aprovizionare;
- platforme pentru detectarea incidentelor, răspunsul la incidente și recuperare, inclusiv instrumente automate de alertare și orchestrare;
- soluții securizate pentru actualizări și managementul patch-urilor, destinate sistemelor încorporate sau dispozitivelor IoT.

NOTĂ IMPORTANTĂ: Achiziția de bunuri va fi evaluată cu atenție de către Comitetul de evaluare pentru a se verifica dacă atât costurile declarate, cât și bunurile care urmează să fie achiziționate sunt coerente cu propunerea de proiect. Exemplele de mai sus nu reprezintă în mod necesar articole care vor fi acceptate automat la depunerea propunerii. Eligibilitatea acestora va depinde de contextul implementării și de relevanța lor în cadrul proiectului propus.