SECURE
Cyber Resilience for SMEs

CRA101: Înțelegerea obligațiilor CRA

31/03/2026

Funded by the European Union

Finanțat de Uniunea Europeană în baza Acordului de Grant (GA) Nr. 101190325. Opiniile și punctele de vedere exprimate aparțin însă exclusiv autorului (autorilor) și nu reflectă neapărat cele ale Uniunii Europene sau ale Centrului European de Competențe Industriale, Tehnologice și de Cercetare în materie de Securitate Cibernetică. Nici Uniunea Europeană și nici autoritatea finanțatoare nu pot fi trase la răspundere pentru acestea

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Proiectul este susținut de Centrul European de Competențe în materie de Securitate Cibernetică și de membrii săi.

DISCLAIMER

Acest document face parte din Livrabilul D4.1 „Ghiduri şi materiale pentru conformitatea IMM-urilor cu CRA" din cadrul Proiectului SECURE. A fost publicat iniţial în octombrie 2025 şi actualizat în martie 2026.

Primul autor: Centrul pentru Securitate Cibernetică din Belgia (CCB)
Al doilea autor: Autoritatea Pentru Digitalizarea României-NCC-RO (ADR-NCC-RO)

Lista Tabelelor și Figurilor

Abrevieri

CE – Conformité Européenne (Conformitate Europeană)

CRA – Cyber Resilience Act (Actul privind Reziliența Cibernetică)

CSIRT – Computer Security Incident Response Team (Echipa de Răspuns la Incidente de Securitate Cibernetică)

CVD – Coordinated Vulnerability Disclosure (Divulgarea Coordonată a Vulnerabilităților)

ENISA – European Union Agency for Cybersecurity (Agenția Uniunii Europene pentru Securitate Cibernetică)

EU / UE – European Union / Uniunea Europeană

EU DoC – European Union Declaration of Conformity (Declarația de Conformitate a Uniunii Europene)

NB – Notified Body (Organism Notificat)

PDE – Product with Digital Elements (Produs cu Elemente Digitale)

SBOM – Software Bill of Materials (Lista de Materiale Software)

SME / IMM – Small and Medium Enterprise (Întreprindere Mică și Mijlocie)

SPOC – Single Point of Contact (Punct Unic de Contact)

Introducere

Actul privind Reziliența Cibernetică (CRA) al Uniunii Europene, Regulamentul (UE) 2024/2847, a fost adoptat cu scopul de a spori pregătirea și reziliența în materie de securitate cibernetică a pieței digitale din UE, în lumina provocărilor cibernetice tot mai mari. Prin introducerea unor reguli armonizate și a unor cerințe minime clare de securitate cibernetică, CRA intenționează să reducă vulnerabilitățile și să protejeze atât consumatorii, cât și companiile. Deși acest regulament de referință a intrat în vigoare în decembrie 2024, acesta optează pentru o implementare etapizată, permițând o perioadă de tranziție și adaptare din 2024 până în 2027.

Mai exact, CRA enumeră obligații pentru producători, importatori și distribuitori de produse cu elemente digitale (PDE-uri). Articolul 13 și Anexa I din CRA enumeră cerințele esențiale de securitate cibernetică pe care producătorii trebuie să le respecte, atât la introducerea PDE-urilor pe piața UE, cât și pe parcursul întregului ciclu de viață al PDE-ului. Partea I a cerințelor din Anexa I se concentrează pe proprietățile PDE-urilor, în timp ce partea a II-a se concentrează pe gestionarea vulnerabilităților. Cu toate acestea, dincolo de Anexa I și Articolul 13 din CRA, sunt impuse și alte cerințe – de exemplu, privind informațiile și instrucțiunile pentru utilizatori (Anexa II), obligațiile de raportare (Articolele 14-17) și conformitatea (Articolele 27-32).
Într-un efort preliminar de a traduce obligațiile legale cheie în îndrumări concrete, acest ghid oferă o imagine de ansamblu simplificată[1] a obligațiilor, împărțită în cinci secțiuni ce trebuie luate cel puțin în considerare. Scopul este de a spori accesibilitatea regulamentului și de a îmbunătăți conștientizarea și înțelegerea la un nivel de bază, în special pentru Întreprinderile Mici și Mijlocii (IMM-uri), în conformitate cu obiectivele proiectului SECURE[2]. Pentru îndrumări tehnice și instrumente privind punerea în aplicare a acestor prevederi în practică, materiale suplimentare sunt puse la dispoziție în depozitul deschis SECURE în mod continuu.

Cronologia CRA:

- Intrarea în vigoare: 10 Decembrie 2024
- Aplicarea obligațiilor de raportare: 11 Septembrie 2026
- Aplicarea deplină a cerințelor CRA: 11 Decembrie 2027

[1] Aceasta este o listă neexhaustivă menită să simplifice obligațiile CRA și nu include excepțiile luate în considerare în cadrul CRA. Sunt incluse doar obligațiile principale pentru a oferi o imagine de ansamblu. Acestea au fost selectate pe baza unei lecturi atente a textului legislativ CRA.

[2] Proiectul „Consolidarea rezilienței cibernetice a IMM-urilor din UE" (SECURE) oferă sprijin financiar și îndrumare pentru IMM-uri pentru a se conforma CRA.

Înțelegerea Obligațiilor CRA - CRA 101

1. Evaluarea Riscurilor de Securitate Cibernetică

Pentru a respecta obligația de a vă asigura că PDE-ul dumneavoastră „a fost proiectat, dezvoltat și produs în conformitate cu cerințele esențiale de securitate cibernetică stabilite în Partea I din Anexa I”[3] – adică garantarea „unui nivel adecvat de securitate cibernetică pe baza riscurilor”[4] – trebuie efectuată o evaluare a riscurilor de securitate cibernetică. Această evaluare trebuie documentată[5] și actualizată periodic pe parcursul așa-numitei „perioade de suport”[6].

Concret, evaluarea riscurilor ar trebui să includă, cel puțin[7]:

1) O **analiză a riscurilor de securitate cibernetică**, luând în considerare:

   - Scopul preconizat al PDE-ului și utilizarea previzibilă;
   - Condițiile de utilizare (de exemplu, mediul operațional, activele care trebuie protejate).

2) O **clarificare, explicație și/sau justificare** a:
   - Aplicării securității prin proiectare (security by design)[8] – adică, cum este aceasta aplicată?
   - Aplicabilității (sau neaplicabilității) cerințelor din Anexa I, Partea I, pentru PDE – adică, sunt aplicabile cerințele de securitate și în ce mod?
   - Aplicării și implementării cerințelor de gestionare a vulnerabilităților[9] – adică, cum sunt aplicate cerințele de gestionare a vulnerabilităților?

Atunci când un PDE conține componente provenite de la terți, CRA așteaptă de la dumneavoastră să exercitați diligența necesară pentru a proteja securitatea cibernetică a produsului final. Acest lucru poate însemna, de exemplu, raportarea unei vulnerabilități pe care ați identificat-o către

[3] Art. 13(1), CRA.
[4] Anexa I, Part I(1), CRA.
[5] Documentația tehnică: clarificată la punctul 5.
[6] Perioada de suport: clarificată la punctul 2
[7] Art. 13(3), CRA.
[8] Annex I, Part I(1), CRA.
[9] Annex I, Part II, CRA

producătorul acelei componente și adresarea ulterioară a acesteia. Pentru a face acest lucru, o Listă de Materiale Software (SBOM)[10] și o politică de divulgare coordonată a vulnerabilităților (CVD) pentru furnizori ar trebui menținute și puse la dispoziția autorităților de supraveghere a pieței, la cererea acestora.

2. Gestionarea vulnerabilităților și actualizările de securitate

După cum se stipulează la Articolul 13(8), producătorii trebuie să se asigure că vulnerabilitățile PDE-ului și ale componentelor sale sunt – „gestionate în mod eficient și în conformitate cu cerințele esențiale stabilite în Partea II din Anexa I”[11] pe parcursul perioadei de suport.

Aceasta înseamnă, printre altele[12]:

1) Identificarea și documentarea vulnerabilităților – adică întocmirea SBOM-ului (cel puțin pentru dependențele de nivel superior) și menținerea acestuia la dispoziție pentru a fi furnizat autorităților de supraveghere a pieței la cerere[13];
2) Adresarea și remedierea vulnerabilităților fără întârziere – adică furnizarea de actualizări de securitate fără întârzieri nejustificate și în mod gratuit (însoțite de mesaje de avertizare/consiliere pentru utilizatori):
    - Fiecare actualizare de securitate lansată în timpul perioadei de suport trebuie să rămână disponibilă timp de cel puțin 10 ani de la lansare, sau pentru restul perioadei de suport, oricare dintre acestea este mai lungă[14].
3) Revizuirea și testarea periodică a securității produsului;
4) Partajarea informațiilor despre vulnerabilitățile remediate (și potențiale), impactul și severitatea acestora, instrucțiunile de remediere pentru utilizatori, adresele de contact pentru raportarea vulnerabilităților, precum și stabilirea și aplicarea unei politici CVD.

„Perioada de suport” menționată mai sus „reflectă perioada de timp în care se preconizează că produsul va fi utilizat”[15] și ar trebui să ia în considerare în mod proporțional așteptările utilizatorilor, natura PDE-ului (scopul) și legislația relevantă a Uniunii.

[10] O înregistrare oficială a detaliilor și a relațiilor din lanțul de aprovizionare ale componentelor incluse în elementele software ale PDE-urilor (Art. 3(39), CRA).

[11] Art. 13(8), CRA.

[12] Annex I, Part II, CRA.

[13] Partajarea acesteia cu utilizatorii este opțională.

[14] Art. 13(9), CRA.

[15] Art. 13(8), CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Concret, atunci când vă definiți perioada de suport, aceasta ar trebui să fie:

- De cel puțin cinci ani (cu excepția cazului în care durata de viață a produsului este mai scurtă de cinci ani, caz în care perioada de suport este egală cu durata de viață a produsului)
- Specificată în mod clar (data de încheiere: luna și anul) la momentul achiziției / pe ambalaj / în format digital (atunci când este atinsă, utilizatorii ar trebui, în mod ideal, să fie notificați)[16].

Determinarea și definirea perioadei de suport trebuie incluse în Documentația Tehnică[17].

3. Informații pentru utilizatori, instrucțiuni și Punctul Unic de Contact

În conformitate cu Articolul 13(14-18) și Anexa II, producătorii trebuie ca, cel puțin, să informeze în mod clar utilizatorii prin includerea, în format tipărit sau digital, a următoarelor:

- Detalii despre producător (nume, denumire comercială înregistrată sau marcă înregistrată, adresă poștală, adresă de e-mail sau contact digital, site web);
- Detalii despre PDE (nume, tip, scopul preconizat, mediul de securitate și proprietățile de securitate, funcționalitățile esențiale, posibilele riscuri de securitate cibernetică, suportul tehnic de securitate oferit, data de încheiere a perioadei de suport);
- Instrucțiuni detaliate sau link către acestea (privind măsurile pentru o utilizare sigură, posibilele efecte asupra securității datelor din cauza modificărilor aduse produsului, instalarea actualizărilor de securitate, scoaterea din funcțiune în condiții de siguranță și eliminarea datelor utilizatorului, setările implicite de instalare a actualizărilor de securitate);
- Un Punct Unic de Contact (SPOC) trebuie desemnat pentru a permite utilizatorilor:
    - Să comunice direct și rapid cu producătorul prin mijloacele lor preferate de comunicare (fără a se limita la instrumente automatizate);
    - Să raporteze vulnerabilități;
    - Să localizeze politica CVD.
- Linkuri (dacă este cazul) către politica CVD, declarația UE de conformitate (EU DoC)[18], SBOM (dacă este pus la dispoziția utilizatorilor).

[16] Art. 13(19), CRA.

[17] Documentația tehnică: clarificată la punctul 5.

[18] EU DoC: clarificată la punctul 5.

Instrucțiunile de utilizare ar trebui să fie disponibile într-o limbă ușor de înțeles, online sau pe suport de hârtie, timp de cel puțin zece ani sau pe durata perioadei de suport (oricare dintre acestea este mai lungă).

4. Obligații de raportare: raportarea vulnerabilităților și a incidentelor

În ceea ce privește raportarea[19], tabelul de mai jos oferă o imagine de ansamblu asupra obligațiilor dumneavoastră. Mai jos sunt oferite clarificări suplimentare.

Tabelul 1:
Raportarea vulnerabilităților și a incidentelor

Raportare	Vulnerabilități	Incidente
Ce trebuie raportat?	***Trebuie:*** *„vulnerabilități exploatate activ”* ***Poate:*** *vulnerabilități (care nu sunt exploatate activ); amenințări cibernetice*	***Trebuie:*** *„incidente grave”* ***Poate:*** *incidente (care nu sunt grave); cvasi-incidente (near misses)*
Cui se raportează?	CSIRT[20] Platforma unică de raportare (ENISA) Utilizatorii afectați	
Cum se raportează?	1) Notificare de alertă timpurie (24h) 2) Notificare de vulnerabilitate (72h) 3) Raport final (14 zile)	1) Notificare de alertă timpurie (24h) 2) Notificare de incident (72h) 3) Raport final (1 lună)

[19] Art. 14-17, CRA.

[20] Art. 3(51), CRA: „CSIRT desemnat drept coordonator” înseamnă un CSIRT desemnat drept coordonator în temeiul articolului 12(1) din Directiva (UE) 2022/2555.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

4.1. Ce trebuie raportat?

Conform definițiilor stabilite la Articolul 3 din CRA:

- O **„vulnerabilitate exploatată activ”** necesită dovezi sigure de exploatare de către un actor rău intenționat într-un sistem, fără permisiunea proprietarului[21];
- Un incident este considerat **„grav”** atunci când[22]:
  - Afectează în mod negativ sau poate afecta capacitatea PDE-ului de a proteja disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor sau a funcțiilor; sau
  - A dus sau poate duce la introducerea/executarea de cod rău intenționat în produs sau în rețelele și sistemele informatice ale unui utilizator.

4.2. Cui se raportează?

Echipa de Răspuns la Incidente de Securitate Cibernetică (CSIRT) către care trebuie transmis raportul este cea din Statul Membru în care producătorul[23]:

- Își are sediul principal; sau, dacă acesta nu poate fi determinat,
- Are sediul cu cel mai mare număr de angajați.

Dacă se află în afara UE, se poate urma un lanț de rezervă care ia în considerare sediul reprezentantului autorizat al producătorului importator distribuitor locul unde se află cel mai mare număr de PDE-uri sau utilizatori.

Fără a aduce atingere mai multor excepții, toate notificările vor trece prin platforma unică de raportare, care urmează să fie înființată și menținută de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), și vor fi diseminate către alte CSIRT-uri și autorități de supraveghere a pieței printr-un punct final de notificare electronică.

[21] Art. 3(42), CRA.

[22] Art. 3(44), CRA; Art. 14(5), CRA.

[23] CSIRT este, de regulă, CERT-ul național: Echipa de Răspuns la Urgențe Informatice (Computer Emergency Response Team).

Utilizatorii afectați (și, acolo unde este cazul, toți utilizatorii) trebuie, de asemenea, să fie notificați cu privire la vulnerabilități/incidente și acțiunile pe care trebuie să le întreprindă, de preferat într-un format citibil de către mașină. CSIRT-urile pot informa utilizatorii dacă producătorul nu face acest lucru[24].

4.3. Cum se raportează?

Există mai multe diferențe în ceea ce privește raportarea vulnerabilităților și a incidentelor.

Vulnerabilități

1) Notificarea de alertă timpurie (early warning): ar trebui trimisă cel târziu în termen de 24 de ore de la luarea la cunoștință și ar trebui să indice, dacă este cazul, Statele Membre în care PDE-ul este disponibil.
2) Notificarea de vulnerabilitate: ar trebui trimisă cel târziu în termen de 72 de ore de la luarea la cunoștință și ar trebui să includă:
    - Informații generale despre PDE;
    - Natura generală a vulnerabilității;
    - Măsuri corective sau de atenuare luate sau care pot fi luate de utilizatori;
    - Sensibilitatea informațiilor notificate.
3) Raportul final: ar trebui trimis nu mai târziu de 14 zile după măsura corectivă/de atenuare și ar trebui să includă:
    - Descrierea – severitatea și impactul;
    - Informații despre actorul rău intenționat, dacă este cazul;
    - Detalii despre actualizarea de securitate sau altă măsură corectivă disponibilă.

Incidente

1) Notificarea de alertă timpurie (early warning): ar trebui trimisă cel târziu în termen de 24 de ore de la luarea la cunoștință și ar trebui să indice:
    - Dacă este cazul, Statele Membre în care PDE-ul este disponibil;
    - Dacă există suspiciunea că a fost cauzat de acte ilegale sau rău intenționate.

[24] Art. 14(8) CRA.

2) **Notificarea de incident:** ar trebui trimisă cel târziu în termen de 72 de ore de la luarea la cunoştinţă şi ar trebui să includă:
    - Informaţii generale despre natura incidentului;
    - Evaluarea iniţială a incidentului;
    - Măsuri corective sau de atenuare luate sau care pot fi luate de utilizatori;
    - Sensibilitatea informaţiilor notificate.

3) **Raportul final:** ar trebui trimis în termen de o lună de la trimiterea notificării incidentului şi ar trebui să includă:
    - Descrierea – severitatea şi impactul;
    - Tipul de ameninţare sau cauza probabilă care a generat incidentul;
    - Măsurile de atenuare aplicate şi în curs de desfăşurare.

5. Evaluarea conformităţii

Înainte ca un PDE să fie introdus pe piaţă, producătorul trebuie să demonstreze că acesta respectă cerinţele esenţiale de securitate cibernetică stabilite în Anexa I din CRA. Acest lucru se realizează prin **procedura de evaluare a conformităţii** aplicabilă categoriei de produse respective.

5.1. Proceduri de evaluare a conformităţii

CRA prevede, printre altele:

- Controlul intern (Modulul A);
- Examinarea UE de tip urmată de conformitatea cu tipul (Modulele B + C);
- Asigurarea totală a calităţii (Modulul H);
- Evaluarea în cadrul unui sistem european de certificare a securităţii cibernetice, acolo unde este cazul.

Standardele armonizate şi specificaţiile comune nu sunt proceduri de conformitate, însă pot sprijini demonstrarea conformităţii.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

5.2. Prezumția de conformitate

Un produs care respectă:

- Standardele armonizate ale căror referințe au fost publicate în Jurnalul Oficial, sau
- Specificațiile comune adoptate de Comisia Europeană

este **prezumat a fi conform**[25] cu cerințele esențiale acoperite de acele standarde sau specificații.

Atunci când astfel de standarde sau specificații nu sunt aplicate (sau sunt aplicate parțial), producătorul trebuie să demonstreze direct conformitatea cu cerințele din Anexa I prin procedura de evaluare a conformității aplicabilă. Acolo unde este relevant, un certificat european de securitate cibernetică poate fi, de asemenea, utilizat pentru a demonstra conformitatea, în limitele prevăzute de CRA.

5.3. Categorii de produse

Procedura de evaluare a conformității care trebuie aplicată depinde de clasificarea PDE-ului în temeiul CRA, specificată în Anexele III și IV din CRA[26]. CRA distinge între produse implicite (default), importante (Clasa I și II) și critice.

În funcție de categorie:

- Controlul intern poate fi suficient;
- Poate fi necesară implicarea unui organism notificat (NB); sau
- Evaluarea în cadrul unui sistem european de certificare poate fi obligatorie sau permisă.

Clasificarea corectă este, prin urmare, decisivă pentru determinarea procedurii aplicabile. O privire de ansamblu asupra procedurii care poate fi aplicată per clasă de produse poate fi găsită în Tabelul 2 de pe pagina următoare.

[25] Art. 27, CRA.

[26] Art. 32, CRA; Anexa VIII, CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Tabelul 2:

Proceduri de evaluare a conformității

	Control intern (modulul A)	Examinare UE de tip urmată de conformitatea cu tipul (Modulele B + C)	Asigurare a totală a calității (modulul H)	Sistem european de certificare a securității cibernetice	Standarde armonizate / Specificații comune[27]
Produse implicite (Default)	X	X	X	X	X Pot oferi suport de conformitate pentru cerințele acoperite
Produse importante Clasa I	X[28]	X	X	X nivel: substanțial[29]	X Pot oferi suport de conformitate pentru cerințele acoperite
Produse importante Clasa II		X	X	X nivel: substanțial[30]	X Pot oferi suport de conformitate pentru cerințele acoperite
Produse critice				X nivel: substanțial	X Pot oferi suport de conformitate pentru cerințele acoperite

5.4. Declarația UE de conformitate (EU DoC)

În urma unei evaluări reușite a conformității, producătorul întocmește o Declarație UE de Conformitate (EU DoC)[31].

27 Standardele armonizate și specificațiile comune nu sunt proceduri, dar pot sprijini demonstrarea conformității.

28 Controlul intern (modulul A) poate fi utilizat numai atunci când sunt aplicate standarde armonizate, specificații comune sau, după caz, un sistem de certificare relevant. În caz contrar, căile aplicabile sunt examinarea UE de tip urmată de conformitatea cu tipul (Modulele B+C) sau asigurarea totală a calității (Modulul H).

29 Dacă, în temeiul Art. 8(1) din CRA, este adoptat un act delegat, sistemul de certificare cibernetică al UE poate fi utilizat. În caz contrar, se revine la regulile aplicabile produselor importante din Clasa II.

30 Se aplică nota de subsol 29.

31 Art. 28, CRA; Anexa V-VI, CRA.

În această declarație, confirmați că PDE-ul respectă cerințele esențiale aplicabile și include elementele obligatorii prevăzute de CRA. Structura model poate fi găsită în Anexa V din CRA. Declarația UE de conformitate simplificată poate fi găsită în Anexa VI. Aceasta trebuie pusă la dispoziție în limbile cerute de Statul Membru în care PDE-ul este introdus pe piață și trebuie să rămână disponibilă pentru perioada prevăzută de lege.

5.5. Marcajul CE

Pentru a permite consumatorilor să identifice PDE-urile care îndeplinesc cerințele CRA și să ia decizii informate atunci când achiziționează și utilizează astfel de produse, un marcaj CE[32] trebuie să fie „aplicat în mod vizibil, lizibil și de neșters”[33] înainte ca PDE-ul să fie introdus pe piață. Acest lucru trebuie făcut pe produsul în sine. Atunci când acest lucru nu este posibil din cauza naturii produsului, marcajul trebuie aplicat pe ambalaj și inclus în declarația UE de conformitate însoțitoare[34] [35]. Marcajul CE indică faptul că produsul este conform cu întreaga legislație aplicabilă a Uniunii care impune marcajul CE, inclusiv CRA.

5.6. Dovedirea conformității prin documentația tehnică

O componentă cheie pentru evaluarea conformității este documentația tehnică. Mandatată de Articolul 31 din CRA și Anexa VII, documentația tehnică este relevantă pentru toate punctele discutate anterior, deoarece trebuie întocmită înainte ca PDE-ul să fie introdus pe piață și actualizată continuu pe parcursul perioadei de suport[36]. Reunind majoritatea obligațiilor CRA, documentația tehnică ar trebui, prin urmare, să includă[37]:

- Descrierea generală a PDE-ului (scopul preconizat, versiunile software care afectează conformitatea, dovezi ale caracteristicilor externe, marcajul și aspectul intern pentru produsele hardware, informații și instrucțiuni pentru utilizatori);
- Descrierea proceselor de proiectare, dezvoltare și producție ale PDE-ului, precum și a proceselor de gestionare a vulnerabilităților (de exemplu, descrierea arhitecturii sistemului, SBOM, politica CVD, procesele de monitorizare etc.)

32 Marcajul Conformité Européenne (Conformitate Europeană).

33 Art. 30(1), CRA.

34 Art. 29-30, CRA.

35 Se aplică reguli suplimentare dacă un Organism Notificat participă la evaluarea conformității.

36 Art. 31(2), CRA.

37 Anexa VII, CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Evaluarea riscurilor de securitate cibernetică;
- Definirea și clarificarea perioadei de suport;
- Standardele armonizate aplicate (sau părți ale acestora);
- Rapoarte de testare a conformității și rapoarte de gestionare a vulnerabilităților;
- O copie a Declarației UE de conformitate (EU DoC).

Un **formular simplificat de documentație** tehnică urmează să fie dezvoltat de Comisia Europeană pentru microîntreprinderi și întreprinderi mici[38]. Mai mult, Articolul 33 stipulează că atât Statele Membre, cât și Comisia Europeană trebuie să ofere **sprijin pentru IMM-uri** – printre altele, sub formă de ghiduri[39] și oportunități de sprijin financiar.

Proiectul SECURE **oferă sprijin financiar IMM-urilor care trebuie să se conformeze CRA și furnizează ghiduri și materiale în mod continuu, menite să ajute IMM-urile în implementarea CRA**, cum ar fi acest ghid CRA101.

[38] Art. 33(5), CRA.

[39] Art. 26, CRA

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Concluzie

În efortul de a oferi o imagine de ansamblu accesibilă a obligațiilor cheie stabilite în CRA, acest ghid se concentrează pe cinci componente ale CRA, care trebuie luate în considerare cel puțin: (1) Evaluarea riscurilor de securitate cibernetică; (2) Gestionarea vulnerabilităților și actualizările de securitate; (3) Informații pentru utilizatori, instrucțiuni și Punctul Unic de Contact; (4) Obligații de raportare: raportarea vulnerabilităților și a incidentelor; (5) Evaluarea conformității. Acesta clarifică elemente precum perioada de suport, declarația UE de conformitate, marcajul CE și documentația tehnică. Având ca scop sprijinirea IMM-urilor în navigarea prin acest cadru juridic complex, ghidul oferă un rezumat al principalelor obligații legale care trebuie înțelese înainte de punerea lor în aplicare. Pentru îndrumări practice privind modul de abordare și implementare a acestor prevederi legale, precum și cu privire la elemente particulare ale CRA (de exemplu, SBOM, managementul vulnerabilităților etc.), ghiduri tehnice și instrumente suplimentare vor deveni disponibile în mod continuu pe depozitul central SECURE, pe măsură ce implementarea CRA avansează. Ca pași următori pentru IMM-uri, se recomandă consultarea celorlalte ghiduri din depozitul SECURE, cum ar fi „Cerințele esențiale de securitate cibernetică ale CRA: Anexa I, Partea I" pentru sugestii și recomandări practice privind fiecare dintre prevederile Anexei I, precum și „Cadrul metodologic de evaluare a conformității CRA" pentru un set de instrumente și o listă de verificare pas cu pas privind conformitatea cu CRA dincolo de Anexa I.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE