CONFIRMATE

CONFormIty assessment, metRics and compliance autoMATion for the cyber resiliencE act

Ghid de conformitate cu Regulamentul UE privind reziliența cibernetică pentru IMM-uri

Data publicării: 30.10.2025
Stare: Final
Versiune: 1.0

Proiectul finanțat prin Acordul de finanțare **nr. 101190193** este susținut de Centrul European de Competență în domeniul securității cibernetice. Opiniile și punctele de vedere exprimate sunt însă ale autorului/autorilor și nu le reflectă neapărat pe cele ale Uniunii Europene sau ale Centrului european de competență în domeniul securității cibernetice. Nici Uniunea Europeană, nici autoritatea care acordă finanțarea nu pot fi considerate responsabile pentru acestea.

Lista modificărilor

Versiune	Data	Descriere	Autor
0.1	07.04.2025	Proiect inițial	CYEN
0.2	27.06.2025	Text suplimentar adăugat	CYEN
0,3	06.08.2025	Prima versiune finalizată, text suplimentar / îndrumări adăugate	CYEN
0.4	03.09.2025	Versiune revizuită de partenerii proiectului, pentru distribuire către evaluatori externi	CYEN
0.5	24.10.2025	Versiune revizuită ținând cont de evaluarea colegială	CYEN
1.0	30.10.2025	Versiunea finală publicată	CYEN

Contribuabili

Rol	Numele contribuitorului	Numele entității - Beneficiar
Responsabil livrabil	Iva Tasheva, Steve Purser, Krasimir Simonski, Azeez Kamal	CYEN
Contribuitor	Christine Demeter, Gabriel Niculescu, Mirabela Săvulescu	DNSC
Colaborator	Andreas Binder	AISEC Fraunhofer
Evaluare inter pares	Harald Fischer	Balena
Evaluare inter pares	Argyro Chatzopoulou et al.	Proiectul CURIUM
Evaluare inter pares	Romain Muguet et al.	Red Alert Labs

Declarație de responsabilitate: Instrumentele Confirmate, inclusiv ghidul de conformitate CRA, sunt destinate exclusiv scopurilor informative și educaționale generale. Acestea oferă o introducere la nivel înalt în procesul de conformitate CRA și nu sunt adaptate circumstanțelor unei organizații, unui produs sau unei situații specifice. Conținutul reflectă experiența și opiniile individuale ale experților, autorilor și evaluatorilor care au contribuit și poate să nu fie exhaustiv, actualizat continuu sau aplicabil în fiecare caz.

Aceste instrumente nu reprezintă consultanță juridică sau de reglementare. CONFIRMATE nu își asumă nicio responsabilitate sau răspundere pentru acțiunile întreprinse pe baza informațiilor furnizate. Utilizatorii rămân singurii responsabili pentru asigurarea conformității cu legile, reglementările și standardele aplicabile.

Deoarece cerințele de reglementare evoluează, vă recomandăm insistent să consultați un profesionist juridic calificat sau un expert în reglementare pentru a obține sfaturi specifice circumstanțelor dvs.

Cuprins

1. Glosar: acronime, termeni și abrevieri

În textul prezentelor orientări apar următorii termeni:

Reprezentant autorizat:	Persoană fizică sau juridică stabilită în Uniune care a primit un mandat scris de la un producător pentru a acționa în numele acestuia în legătură cu sarcini specificate.
Marcajul CE:	Marcaj prin care un producător indică faptul că un produs cu elemente digitale și procesele puse în aplicare de producător sunt în conformitate cu cerințele esențiale de securitate cibernetică prevăzute în anexa I la CRA și în alte acte legislative de armonizare ale Uniunii care prevăd aplicarea acestuia.
Declarație de conformitate (DoC):	Un document legal, întocmit de producător, care atestă că un produs îndeplinește cerințele esențiale aplicabile din CRA. Acesta trebuie pus la dispoziția autorităților competente, precum și a utilizatorilor, ca parte a documentației tehnice.
Evaluarea conformității:	Procesul de verificare a îndeplinirii cerințelor esențiale de securitate cibernetică prevăzute în anexa I la CRA.
Standard armonizat:	O specificație tehnică elaborată de o organizație europeană de standardizare (ESO) la cererea Comisiei Europene pentru a contribui la punerea în aplicare a legislației europene. Acestea sunt standarde europene recunoscute oficial care conferă prezumția de conformitate cu cerințele legale specifice din legislația UE.
Incident:	Un eveniment care afectează negativ sau poate afecta negativ capacitatea unui produs cu elemente digitale de a proteja disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor sau funcțiilor, ori a serviciilor oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora.
Distribuitor	O persoană fizică sau juridică din lanțul de aprovizionare, alta decât producătorul sau importatorul, care pune la dispoziție pe piața Uniunii un produs cu elemente digitale fără a afecta proprietățile acestuia.
Importator	Persoană fizică sau juridică stabilită în Uniune care introduce pe piață un produs cu elemente digitale care poartă numele sau marca comercială a unui producător stabilit în afara Uniunii.
Producător	Persoană fizică sau juridică care dezvoltă sau fabrică produse cu elemente digitale sau care dispune de produse cu elemente digitale proiectate, dezvoltate sau fabricate și le comercializează sub numele sau marca sa comercială, fie contra cost, fie în scopul monetizării, fie gratuit.

Noul cadru legislativ (NLF):	Reglementări care stabilesc cerințe structurate și armonizate privind modul în care se evaluează conformitatea produselor înainte ca acestea să fie introduse pe piața UE.
Produs cu elemente digitale (PDE):	Un produs software sau hardware și soluțiile sale de prelucrare a datelor la distanță, inclusiv componentele software sau hardware introduse pe piață separat.
IMM-uri:	Categoria întreprinderilor mici și mijlocii (IMM-uri) este alcătuită din întreprinderi care angajează mai puțin de 250 de persoane și care au o cifră de afaceri anuală de maximum 50 de milioane EUR și/sau un bilanț anual total de maximum 43 de milioane EUR. În cadrul categoriei IMM-urilor, întreprinderea mică este definită ca o întreprindere care are mai puțin de 50 de angajați și a cărei cifră de afaceri anuală și/sau bilanț anual nu depășesc 10 milioane EUR, în timp ce pentru o microîntreprindere, aceste praguri sunt mai puțin de 10 angajați și mai puțin de 2 milioane EUR.
Lista componentelor software:	O evidență formală care conține detalii și relațiile din lanțul de aprovizionare ale componentelor incluse în elementele software ale unui produs cu elemente digitale.
Perioada de asistență:	Perioada în care un producător are obligația de a se asigura că vulnerabilitățile unui produs cu elemente digitale sunt gestionate în mod eficient și în conformitate cu cerințele esențiale de securitate cibernetică prevăzute în partea II din anexa I la CRA.
Vulnerabilitate:	Slăbiciune, defect sau punct slab, o susceptibilitate sau o deficiență a unor produse cu elemente digitale care poate fi exploatat de o amenințare cibernetică. - O vulnerabilitate exploatabilă este o vulnerabilitate care poate fi utilizată în mod eficient de un adversar în condiții operaționale practice; - O vulnerabilitate exploatată în mod activ este o vulnerabilitate pentru care există dovezi fiabile că un actor rău intenționat a exploatat-o într-un sistem fără permisiunea proprietarului sistemului.

2. Introducere

Despre proiectul CONFIRMATE

CONFIRMATE este un proiect inovator cofinanțat de Uniunea Europeană (UE) și Centrul European de Competențe în domeniul Securității Cibernetice (ECCC), conceput pentru a ajuta IMM-urile din sectorul manufacturier să se mențină la curent cu evoluția reglementărilor în materie de securitate cibernetică. Prin simplificarea conformității cu Regulamentul UE privind reziliența cibernetică (Cyber Resilience Act - CRA), CONFIRMATE oferă instrumente open-source, formare practică și metode standardizate care fac conformitatea cu CRA mai accesibilă, mai eficientă și mai rentabilă.

Numele proiectului provine de la Conformity Assessment, Metrics, and Automation for the Cyber Resilience Act (Evaluarea conformității, metrici și automatizare pentru Regulamentul UE privind reziliența cibernetică). Bazat pe cadrul open-source Clouditor, CONFIRMATE oferă decompoziție automată a serviciilor și vizualizări ale conformității, rezultate clare ale evaluării, o metodologie robustă de testare a penetrării, module de formare multilingve în domeniul securității cibernetice[1] și un ghid cuprinzător de conformitate cu CRA (acest document). A se vedea materialele publicate în anexa E.

Reunind parteneri de frunte, printre care CYEN, Fraunhofer AISEC, ITKAM și Directoratul Națională de Securitate Cibernetică (DNSC) din România, CONFIRMATE oferă IMM-urilor cunoștințele și resursele necesare pentru a îndeplini cu încredere cerințele esențiale de securitate cibernetică și pentru a asigura reziliența produselor lor digitale. Alte proiecte UE în curs de desfășurare și conformitatea IMM-urilor cu CRA sunt enumerate în anexa F a prezentului ghid.

2.1 Scopul și publicul țintă al acestui ghid

Ghidul de conformitate este o resursă gratuită dedicată sprijinirii IMM-urile din sectorul manufacturier din UE în înțelegerea cerințelor esențiale de securitate cibernetică ale Regulamentul UE privind reziliența cibernetică (CRA)[2] . Ghidul este conceput special pentru a oferi o imagine de ansamblu asupra cerințelor de conformitate și pentru a sprijini IMM-urile în transformarea așteptărilor sale în pași concreți și ușor de înțeles. Acesta este adaptat nevoilor și provocărilor specifice cu care se confruntă IMM-urile din sectorul de producție. Redactat inițial în limba engleză, ghidul va fi tradus în patru limbi

[1] Vedeți videoclipul introductiv pe YouTube: https://youtu.be/QeIjDeVvbL0
[2] Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului din 23 octombrie 2024: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

europene: germană, franceză, italiană și română, ajungând la peste 60% din populația UE.

Ghidul oferă o imagine de ansamblu cuprinzătoare asupra Regulamentului UE privind reziliența cibernetică (CRA), acoperind aspecte cheie precum rolurile și responsabilitățile, cerințele esențiale de securitate cibernetică, procedurile de evaluare a conformității și raportarea incidentelor cu obligații post-comercializare. De asemenea, oferă pași practici pentru IMM-uri în vederea implementării CRA, împreună cu sugestii de instrumente, șabloane și resurse de sprijin pentru a le îmbunătăți postura de securitate și a sprijini îmbunătățirea continuă.

Scopul principal al ghidului este de a împuternici IMM-urile, oferindu-le cunoștințele și instrumentele necesare pentru a atinge și menține conformitatea cu CRA. Acesta vizează reducerea complexității procesului de navigare în cerințele de reglementare, permițând întreprinderilor să își îndeplinească cu încredere obligațiile, concentrându-se în același timp pe operațiunile lor de bază. În plus, ghidul servește la evidențierea importanței pentru IMM-uri a gestionării riscurilor de securitate cibernetică, a protejării reputației lor și a asigurării securității și fiabilității produselor lor digitale. În cele din urmă, acesta va oferi IMM-urilor cunoștințele și măsurile practice necesare pentru a îmbunătăți reziliența cibernetică pe întreaga durată de viață a produselor.

Publicul țintă: Ghidul este special conceput pentru IMM-urile europene care dezvoltă, produc sau comercializează produse cu elemente digitale. Aceste întreprinderi nu dispun adesea de resursele și expertiza extinse ale organizațiilor mai mari, ceea ce face ca respectarea reglementărilor complexe, precum CRA, să reprezinte o provocare semnificativă. Concentrându-se asupra IMM-urilor, ghidul urmărește să abordeze provocările specifice ale acestora, cum ar fi bugetele limitate, echipele mai mici și nevoia de soluții practice și scalabile.

În ciuda faptului că demonstrează o înțelegere a provocărilor menționate mai sus cu care se confruntă IMM-urile, obligațiile CRA sunt aceleași pentru IMM-uri și pentru întreprinderile mari, cu câteva excepții, și anume șabloanele de documentație simplificate (documentația tehnică și declarația de conformitate) și orientările prioritare, care sunt abordate și în acest ghid.

În acest sens, cu excepția cazului în care se menționează explicit, toate orientările din acest document se aplică IMM-urilor.

Pe scurt, acest ghid de conformitate este o resursă valoroasă pentru IMM-urile producătoare din UE, oferindu-le claritate, încredere și instrumente practice pentru a naviga printre cerințele Regulamentului UE privind reziliența cibernetică. Acesta nu numai că sprijină conformitatea, ci și promovează o cultură a maturității în materie de

securitate cibernetică, ajutând IMM-urile să își protejeze produsele, clienții și reputația într-o piață din ce în ce mai digitalizată.

2.2 Întrebări și răspunsuri cheie privind Regulamentul UE privind reziliența cibernetică (CRA)

Î1. Ce este Regulamentul UE privind reziliența cibernetică (CRA)?
CRA este un regulament al UE care vizează asigurarea securității cibernetice a produselor cu elemente digitale (PDE), cum ar fi dispozitivele conectate și software-ul. Acesta introduce cerințe de securitate obligatorii pe tot parcursul ciclului de viață al produsului, de la proiectare până la asistența post-vânzare.

Deși este larg recunoscută, definiția CRA a „produselor cu elemente digitale, PDE" merită detaliată, deoarece este legată de faptul dacă produsele IMM-urilor trebuie să îndeplinească cerințele sale.

Prin definiție, PDE include produse software sau hardware și soluțiile sale de procesare a datelor la distanță. În ceea ce privește software-ul, nu există loc pentru interpretări, deoarece acesta este ușor de recunoscut ca cod de programare. În ceea ce privește hardware-ul, însă, există o clarificare conform căreia acesta trebuie să fie capabil să proceseze, să stocheze sau să transmită date digitale, precum și să fie introdus pe piață separat, chiar dacă face parte dintr-un lanț de aprovizionare ca componentă a unui alt produs.

Î2. CRA se aplică produselor noastre?
Dacă compania dvs. produce sau comercializează pe piața UE produse cu elemente digitale (de exemplu, dispozitive IoT, software încorporat, mașini industriale cu interfețe de rețea), atunci da, CRA se aplică probabil. Există excepții pentru produsele deja reglementate, cum ar fi dispozitivele medicale, vehiculele ușoare, aviația, produsele concepute exclusiv pentru uz militar, securitate națională, utilizarea informațiilor clasificate.

Î3. Sunt afectat de CRA?
Dacă sunteți producător, importator, distribuitor și administrator open-source al unui PDE introdus pe piața UE, atunci aveți obligații specifice în temeiul CRA.

Î4. Care sunt principalele obligații ale producătorilor?

- Efectuarea și documentarea **evaluărilor riscurilor de securitate cibernetică,** inclusiv a riscurilor legate de lanțul de aprovizionare
- Asigurarea practicilor **de securitate prin proiectare** și **securitate implicită**
- Implementarea proceselor **de gestionare a vulnerabilităților**, inclusiv raportarea și toleranța zero pentru vulnerabilitățile exploatate în mod activ și cunoscute de public.
- Furnizarea de **actualizări de securitate** pe durata ciclului de viață al produsului

- **Realizarea procedurilor de evaluare a conformității** adaptate clasei de produse.
- Crearea și menținerea **documentației tehnice, a fișierelor cu informații pentru utilizatori, a declarației de conformitate UE** (în limbile țării de comercializare)

Î5. Când intră în vigoare CRA?
CRA va fi aplicată într-o abordare etapizată. Datele cheie pentru producători sunt:

➔ **11 septembrie 2026,** când devin aplicabile obligațiile de raportare a vulnerabilităților și incidentelor de securitate

➔ **11 decembrie 2027,** când va avea loc aplicarea integrală a CRA.

Î6. Care sunt sancțiunile pentru nerespectarea prevederilor?
Nerespectarea poate duce la amenzi de până la **15 milioane de euro sau 2,5% din cifra de afaceri anuală globală**, oricare dintre acestea este mai mare. Retragerea de pe piață și afectarea reputației sunt, de asemenea, riscuri.

Î7. Ce ar trebui să facă producătorii în acest moment?
- **Identificați produsele din portofoliu** care intră în domeniul CRA
- Începeți **evaluările riscurilor de securitate cibernetică și analiza lacunelor**
- Actualizați **proiectarea, documentația tehnică și politicile de asistență**
- **Luați în considerare alinierea la standardele de securitate cibernetică** (de exemplu, EUCC, ISO/IEC 2700x, ETSI EN 303 645)

2.3 Contextul și obiectivul Regulamentului UE privind reziliența cibernetică (CRA)

Regulamentul UE privind reziliența cibernetică vine ca o continuare a primei legislații orizontale privind siguranța produselor, Directiva privind echipamentele radio (RED)[3] , care a introdus primele cerințe de securitate cibernetică pentru o gamă largă de produse vândute în UE, în special pentru dispozitivele conectate la internet și cele care gestionează date cu caracter personal, care devin obligatorii începând cu 1 august 2025. Aceste cerințe, prevăzute la articolul 3 alineatul (3) din RED, vizează îmbunătățirea siguranței și securității utilizatorilor și rețelelor prin abordarea protecției rețelelor, confidențialității datelor și prevenirii fraudei. CRA este, de asemenea, legată de Directiva privind răspunderea pentru produse (PLD)[4] , care abordează răspunderea pentru produsele defecte, inclusiv cele cu elemente digitale.

[3] Directiva 2014/53/UE a Parlamentului European și a Consiliului din 16 aprilie 2014: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0053
[4] Directiva (UE) 2024/2853 a Parlamentului European și a Consiliului din 23 octombrie 2024: https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng

Obiectivele Regulamentului UE privind reziliența cibernetică (CRA) sunt *„îmbunătățirea standardelor de securitate cibernetică ale produselor care conțin o componentă digitală, impunând producătorilor și comercianților cu amănuntul să asigure securitatea cibernetică pe tot parcursul ciclului de viață al produselor lor (...) Regulamentul EU privind reziliența cibernetică abordează nivelul inadecvat de securitate cibernetică al multor produse și lipsa actualizărilor de securitate în timp util pentru produse și software”*[5] . Aceasta vizează stabilirea unui nivel ridicat și uniform de securitate cibernetică prin stabilirea unor cerințe clare pentru producători, dezvoltatori, importatori și distribuitori, promovând în același timp transparența în ceea ce privește riscurile de securitate cibernetică.

„Regulamentul UE privind reziliența cibernetică va asigura că:

- *produsele cu fir și fără fir conectate la internet și software-ul introdus pe piața UE să fie mai sigure;*
- *producătorii să rămână responsabili pentru securitatea cibernetică a unui produs pe toată durata ciclului său de viață;*
- *consumatorii să fie informați în mod corespunzător cu privire la securitatea cibernetică a produselor pe care le cumpără și le utilizează.”*[6]

Aceasta „introduce cerințe obligatorii de securitate cibernetică pentru producători și comercianți cu amănuntul, care reglementează planificarea, proiectarea, dezvoltarea și întreținerea acestor produse”[7] . Aceste obligații trebuie îndeplinite în fiecare etapă a lanțului valoric. Aceasta pune accentul pe principiile securității prin proiectare, evaluările de conformitate și raportarea incidentelor cibernetice și a vulnerabilităților exploatate în mod activ, pentru a crea un ecosistem digital mai sigur.

Impactul CRA nu se limitează la un sector specific, ceea ce permite un impact mai larg și stabilirea unui nivel minim de securitate acceptabil pentru produsele vândute în întreaga UE. Astfel, se contribuie la o mai bună reziliență cibernetică. În special pentru IMM-uri, CRA oferă un cadru pentru integrarea securității cibernetice în procesele lor, ajutându-le să concureze pe o piață sigură și de încredere.

Legătura și relația dintre CRA și alte reglementări relevante ale UE în materie de siguranță și securitate sunt descrise în apendicele G Relația cu alte acte legislative ale UE.

[5] Comisia Europeană (2025) Regulamentul UE privind reziliența cibernetică, accesată la 14 aprilie 2025 aici: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[6] Comisia Europeană (2025) Regulamentul UE privind reziliența cibernetică – Întrebări și răspunsuri, accesată la 14 aprilie 2025 aici: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5375
[7] Comisia Europeană (2025) Regulamentul UE privind reziliența cibernetică, accesată la 14 aprilie 2025 aici: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

2.4 Domeniul de aplicare și punerea în aplicare a Regulamentului UE privind reziliența cibernetică (CRA)

Domeniu de aplicare: CRA se aplică tuturor produselor cu elemente digitale introduse pe piața UE (adică vândute separat, nu ca parte a unui serviciu), *„conectate direct sau indirect la un alt dispozitiv sau rețea, cu excepția unor excluderi specificate, cum ar fi anumite produse software sau servicii open-source care sunt deja acoperite de normele existente, cum este cazul dispozitivelor medicale, aviației și automobilelor. Produsele vor purta marcajul CE pentru a indica faptul că respectă cerințele CRA."*[8] Obligațiile se extind pe întregul ciclu de viață al produsului, de la concepție, proiectare, producție și întreținere, până la eliminare.

Merită clarificat faptul că, dacă un PDE nu este conectat direct la o rețea sau la un alt sistem electronic de informații, acesta poate totuși să propage indirect o amenințare către o anumită țintă prin fișiere infectate, unități flash etc. (considerentul 9). Poate fi vorba de un dispozitiv autonom, cum ar fi o încuietoare inteligentă, o jucărie și altele (considerentul 10).

„Pe baza noului cadru legislativ pentru legislația privind produsele în UE, producătorii ar urma un proces de evaluare a conformității pentru a demonstra dacă cerințele specificate referitoare la un produs au fost îndeplinite. Acest lucru s-ar putea realiza prin autoevaluare sau prin evaluarea conformității de către o terță parte, în funcție de nivelul de risc asociat produsului în cauză."[9]

CRA clasifică produsele cu elemente digitale în patru categorii (implicite, importante clasa I, importante clasa II, critice). Toate categoriile de produse trebuie să implementeze aceleași cerințe esențiale de securitate cibernetică (stabilite de regulament, care sunt discutate în secțiunea 3 a acestui document), dar să asigure un nivel adecvat de protecție în funcție de risc și să respecte diferite proceduri de aplicare (evaluare a conformității):

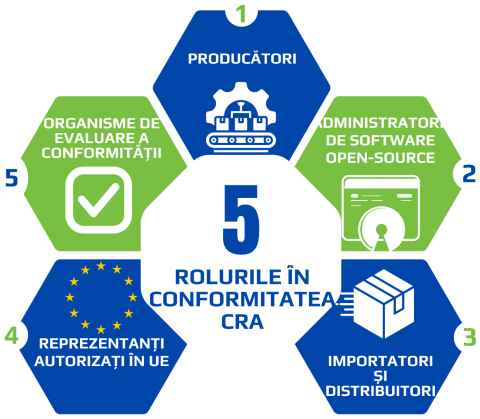
- **Produsele implicite cu elemente digitale** reprezintă aproximativ 90 % din toate produsele cu elemente digitale. Acestea trebuie să îndeplinească cerințele esențiale de securitate cibernetică, afirmând acest lucru prin autoevaluare și declarație de conformitate.
- **Produsele importante cu elemente digitale** sunt enumerate în anexa III și împărțite în două categorii - clasa I și clasa II**.** Se consideră că aceste produse îndeplinesc funcții critice pentru securitatea cibernetică a altor produse, rețele sau servicii și, în acest sens, prezintă un risc semnificativ. Pe lângă îndeplinirea

[8] ibid
[9] Comisia Europeană (2025) Regulamentul UE privind reziliența cibernetică, accesată la 14 aprilie 2025 aici: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

cerințelor esențiale de securitate cibernetică, există cerințe mai stricte de verificare a securității cibernetice pentru acestea înainte de a fi introduse pe piață.

- **Produsele critice cu elemente digitale** sunt enumerate în anexa IV. Lista produselor este foarte limitată, acestea fiind considerate cele mai riscante, și vor fi obligate să obțină un certificat european de securitate cibernetică la un nivel de asigurare cel puțin „substanțial” în cadrul unui sistem european de certificare a securității cibernetice adoptat în conformitate cu Regulamentul (UE) 2019/881.

3. Roluri și responsabilități



Obligațiile CRA vizează o serie de actori din lanțul de aprovizionare al unui produs, fără a face distincție între dimensiune sau origine, ci concentrându-se pe rolul persoanei juridice sau fizice în raport cu PDE din domeniul de aplicare. Cu toate acestea, vor fi publicate orientări (astfel cum sunt prezentate în prezentul document) și modele simplificate pentru a permite în special IMM-urilor să își îndeplinească în mod eficient și eficace rolurile și responsabilitățile.

CRA definește rolurile specifice și responsabilitățile respective după cum urmează:

3.1 Producători

Producătorul joacă un rol major în securitatea cibernetică a produselor cu elemente digitale în etapele de proiectare, dezvoltare, producție și asistență. Ca atare, producătorul este profilul de întreprindere principal în CRA, având întreaga serie de responsabilități (adică punerea în aplicare a cerințelor esențiale de securitate cibernetică și a procedurilor de evaluare a conformității).

CRA definește un producător ca *„o persoană fizică sau juridică care dezvoltă sau fabrică produse cu elemente digitale sau care are produse cu elemente digitale proiectate, dezvoltate sau fabricate și le comercializează sub numele sau marca sa comercială, fie contra cost, fie în scopul monetizării, fie gratuit*".

Această definiție implică faptul că toate etapele ciclului de viață al unui produs sunt realizate de un singur producător, care poartă întreaga responsabilitate pentru securitatea cibernetică a produsului. În practică, după cum știm, linia de producție este întotdeauna mult mai complexă, implicând lanțuri de aprovizionare, terți și alți actori, ceea ce, însă, nu duce la o responsabilitate partajată. Pentru fiecare etapă a ciclului de viață al produsului există cerințe specifice de securitate cibernetică pentru fiecare activitate, etapă și operațiune în parte. Responsabilitățile producătorului nu se încheie odată cu introducerea PDE pe piață.

Obligațiile producătorilor (a se vedea tabelul 1) sunt rezumate în articolele 13 și 14 din CRA din textul oficial și sunt interpretate în prezentul document.

Obligație	Activitate
Implementarea cerințelor esențiale de securitate cibernetică din CRA	Atunci când introduc pe piață un produs cu elemente digitale, producătorii se asigură că acesta a fost proiectat, dezvoltat și produs în conformitate cu cerințele esențiale de securitate cibernetică prevăzute în partea I din anexa I.
Evaluarea periodică a riscurilor	Efectuarea și actualizarea periodică a evaluărilor riscurilor de securitate cibernetică pentru produse și lanțul de aprovizionare. Luarea în considerare a rezultatelor evaluării pentru planificarea, proiectarea, dezvoltarea, producția, livrarea și întreținerea PDE, în vederea minimizării riscurilor de securitate cibernetică, prevenirii incidentelor și minimizării impactului acestora, inclusiv în ceea ce privește sănătatea și siguranța utilizatorilor. Evaluarea riscurilor de securitate cibernetică indică modul în care sunt implementate cerințele esențiale de securitate cibernetică (inclusiv gestionarea vulnerabilităților).

Securitate prin proiectare și implicit	Asigurați-vă că produsele sunt proiectate în mod sigur și sunt livrate cu configurații implicite sigure.
Gestionarea vulnerabilităților	Implementați procese clare, cu toleranță zero pentru vulnerabilitățile cunoscute public și exploatate în mod activ.
Actualizări de securitate	Oferiți actualizări de securitate gratuite și în timp util pe tot parcursul ciclului de viață al produsului, separat de actualizările de funcționalități.
Conformitate și marcaj CE	Efectuați evaluarea conformității (autoevaluare sau evaluare de către terți) și aplicați marcajul CE.
Documentație și DoC	Creați și mențineți documentația tehnică și Declarația de conformitate UE (în limbile pieței țintă).
Raportare	Raportați vulnerabilitățile exploatate în mod activ și incidentele semnificative cu impact asupra securității, simultan către CSIRT și ENISA, prin intermediul platformei unice de raportare (UE), după cum urmează:
	- Avertisment timpuriu: în termen de 24 de ore
	- Raport inițial: în termen de 72 de ore
	- Raport final: în termen de 14 zile (vulnerabilitate) / 1 lună (incident)
	Informați utilizatorii afectați ai produsului cu elemente digitale

Tabelul 1: Obligațiile producătorilor

Secțiunea 3 din prezentul document detaliază cerințele esențiale de securitate cibernetică stabilite de anexa I la regulament, rezumate aici după cum urmează:

- Efectuarea și documentarea **evaluării riscurilor de securitate cibernetică,** inclusiv a riscurilor legate de lanțul de aprovizionare**;**
- Asigurarea practicilor **de securitate prin proiectare** și **securitate implicită**
- Implementarea proceselor **de gestionare a vulnerabilităților**, inclusiv raportarea și toleranța zero pentru vulnerabilitățile exploatate în mod activ cunoscute de public.
- Furnizarea de **actualizări de securitate** pe durata ciclului de viață al produsului
- Efectuarea procedurilor **de evaluare a conformității** adaptate clasei de produse.
- Crearea și menținerea **documentației tehnice, a fișierelor cu informații pentru utilizatori, a declarației de conformitate UE** (în limbile țării în care este comercializat produsul, inclusiv informațiile necesare. Un model simplificat al declarației de conformitate este disponibil pentru IMM-uri și poate fi găsit în anexa VI la CRA și în anexa I la prezentul document).

IMM-urile recunoscute ca producători trebuie informate că CRA introduce raportarea obligatorie a vulnerabilităților exploatate în mod activ și a incidentelor grave atunci când

producătorul ia cunoștință de acestea. Un incident este considerat grav atunci când este cauzat de sau poate introduce coduri malicioase sau afectează disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor sau funcțiilor sensibile sau importante ale PDE.

Deși microîntreprinderile și întreprinderile mici nu sunt supuse unor amenzi administrative dacă nu respectă termenul de avertizare timpurie de 24 de ore, li se recomandă să facă acest lucru cât mai curând posibil. Obligațiile de raportare sunt discutate în detaliu în capitolul 6.

3.2 Administratorii de software open-source

Rolul administratorului de software open-source este foarte tipic pentru IMM-uri, deoarece conceptul de cod liber și open-source provine din IMM-uri și din societatea liber-profesionistă și are un caracter comunitar, mai degrabă decât comercial. Prin urmare, introducerea obligațiilor pentru furnizorii de software open-source este dificil de definit atunci când aceștia fac parte din lanțul de aprovizionare pentru fabricarea produselor cu elemente digitale.

Definiția administratorului de software open-source califică PDE-ul acestora ca software liber și open-source, așteptându-se ca acesta să fie susținut în mod sistematic și continuu, precum și subliniind faptul că este destinat activităților comerciale.
Furnizorii de software open source nu sunt clasificați ca producători de către CRA, cu excepția cazului în care desfășoară activități comerciale cu software open source, cum ar fi taxarea pentru software-ul în sine, furnizarea de asistență tehnică contra cost sau monetizarea prin servicii conexe. Acest lucru este clar menționat în considerentul 18 al CRA: „numai software-ul liber și open-source pus la dispoziție pe piață și, prin urmare, furnizat pentru distribuție sau utilizare în cadrul unei activități comerciale, ar trebui să intre în domeniul de aplicare al prezentului regulament”.

Deși CRA nu stabilește amenzi administrative pentru administratorii de software open source, aceștia sunt supuși unui regim de reglementare ușor, cu obligații enumerate la articolul 24 din CRA și rezumate în tabelul 2 de mai jos.

Obligație	Activitate
Politica de securitate cibernetică și de gestionare a vulnerabilităților	Punerea în aplicare și documentarea unei politici de securitate cibernetică pentru a promova dezvoltarea unui PDE sigur, precum și gestionarea eficientă a vulnerabilităților de către dezvoltatorii acelui produs, încurajând raportarea voluntară a vulnerabilităților și schimbul de informații privind vulnerabilitățile descoperite în cadrul comunității open-source.

Cooperare	Cooperarea cu autoritățile de supraveghere a pieței, la cererea acestora, în vederea atenuării riscurilor de securitate cibernetică prezentate de produsele software gratuite și open-source.
Notificare	Notificați autoritățile competente și utilizatorii afectați (sau toți utilizatorii) cu privire la vulnerabilitățile exploatate în mod activ (dacă sunt implicați în dezvoltarea produsului) și incidentele grave care au un impact asupra securității produselor cu elemente digitale, în măsura în care acestea afectează rețelele și sistemele informatice furnizate de administratorii de software open-source pentru dezvoltarea acestor produse.
	Comunicați, dacă este necesar, orice măsuri de atenuare a riscurilor și măsuri corective pe care utilizatorii le pot implementa pentru a atenua impactul vulnerabilității sau incidentului respectiv.

Tabelul 2: Obligațiile administratorilor de software open-source

Articolele 21 și 22 din CRA tratează cazurile în care obligațiile producătorilor se aplică și altor părți. Prin urmare, aceste orientări sunt relevante și în aceste cazuri.

3.3 Importatori și distribuitori

IMM-urile pot fi, de asemenea, importatori sau distribuitori de produse cu elemente digitale. Pentru aceste roluri, CRA stabilește obligații specifice în articolele 19 și, respectiv, 20, cum ar fi respectarea cerințelor esențiale de securitate cibernetică discutate în capitolul 3 de mai jos și asumarea unor obligații ale producătorului.

Un importator este definit ca *„o persoană fizică sau juridică stabilită în Uniune care introduce pe piață un produs cu elemente digitale care poartă numele sau marca comercială a unei persoane fizice sau juridice stabilite în afara Uniunii”.*

Un distribuitor, pe de altă parte, este *„o persoană fizică sau juridică din lanțul de aprovizionare, alta decât producătorul sau importatorul, care pune la dispoziție pe piața Uniunii un produs cu elemente digitale fără a afecta proprietățile acestuia”.*

Deși aceste orientări au fost elaborate având în vedere producătorii, ele pot fi utilizate în mod rezonabil atât de importatori, cât și de distribuitori, cu condiția să se înțeleagă diferențele dintre obligațiile care se aplică acestor grupuri.

Obligațiile principale atât pentru importatori (articolul 19), cât și pentru distribuitori (articolul 20) sunt rezumate în tabelul 3 de mai jos:

Obligație	Activitate	Actor	
		Importator	Distribuitor
Să introducă pe piața UE numai produse conforme cu	Nu introduceți pe piața UE produse care nu sunt conforme cu CRA;	✅	✅

CRA			
Gestionați produsele neconforme	Asigurați-vă că se efectuează corecții sau retragerea/rechemarea produselor dacă suspectați că acestea nu sunt conforme cu CRA sau cu anexa I la acesta - Cerințe esențiale de securitate cibernetică;	✅	✅
Raportați	Informați producătorul și autoritățile de supraveghere a pieței, fără întârzieri nejustificate, în cazul unui risc semnificativ pentru securitatea cibernetică prezentat de PDE;	✅	✅
	Informați producătorul cu privire la orice vulnerabilitate a produsului;	✅	✅
	Informați autoritățile de supraveghere a pieței și, în măsura posibilului, utilizatorii, în cazul în care producătorul respectivului produs și-a încetat activitatea și, prin urmare, nu este în măsură să își îndeplinească obligațiile care îi revin în temeiul CRA.	✅	✅
Autoidentificare	*Să plaseze datele de contact pe PDE sau pe documentația care însoțește produsul, într-o limbă ușor de înțeles de către utilizatori și autoritățile de supraveghere a pieței.*	✅	
Păstrați documentele de conformitate	*Păstrați o copie a declarației de conformitate UE la dispoziția autorităților de supraveghere a pieței timp de cel puțin 10 ani.*	✅	
Asigurați-vă	Înainte de introducerea unui produs pe piață:		
	(a) că au fost efectuate procedurile corespunzătoare de evaluare a conformității[10] *;*	✅	
	(b) producătorul a întocmit documentația tehnică;	✅	
	(c) PDE poartă marcajul CE și este însoțit de declarația de conformitate UE, precum și de informațiile și instrucțiunile pentru utilizator prevăzute în anexa II, într-o limbă ușor de înțeles de către utilizatori și autoritățile de supraveghere a pieței[11] *;*	✅	
	(d) PDE sau documentația acestuia poartă identificarea produsului, a producătorului și a perioadei de asistență[12] *.*	✅	
	Producătorul și importatorul și-au îndeplinit obligațiile și au furnizat distribuitorului toate documentele necesare.		✅

Tabelul 3: Obligațiile importatorilor și distribuitorilor

În plus, articolul 21 identifică circumstanțele în care obligațiile care se aplică producătorilor se aplică și importatorilor și distribuitorilor. Acest lucru se întâmplă atunci când importatorul sau distribuitorul introduce un PDE pe piață sub numele sau marca sa comercială sau efectuează o modificare substanțială a unui PDE deja introdus pe piață.

[10] *Conform articolului 32*
[11] *Astfel cum se prevede la articolul 30 și la articolul 13 alineatul (20) în consecință*
[12] *Conform articolului 13 alineatele (15), (16) și (19)*

3.4 Alte persoane fizice sau juridice (articolul 22)

Articolul 22 se referă la cazul în care o persoană fizică sau juridică (alta decât producătorul, importatorul sau distribuitorul) efectuează o modificare substanțială a unui PDE și pune produsul respectiv la dispoziție pe piață. În acest caz, entitatea în cauză este considerată producător.

3.5 Reprezentanți autorizați în UE

Un alt rol în care IMM-urile pot fi recunoscute este cel de reprezentant autorizat al producătorului. Acesta este un rol derivat din cel al producătorului și este definit într-un mandat special prin care producătorul numește reprezentantul autorizat. Mandatul poate include oricare dintre obligațiile producătorului, cu excepția celor specificate în mod explicit de CRA la articolul 18, care sunt în mare parte legate de securitatea cibernetică în etapele de proiectare, dezvoltare și producție. Cu toate acestea, în ceea ce privește cerințele CRA privind conformitatea produsului cu normele de securitate cibernetică atunci când se află pe piață, reprezentantul trebuie să coopereze cu autoritățile care exercită controlul asupra PDE pe care le reprezintă.

Producătorii pot alege să desemneze un reprezentant autorizat pentru a îndeplini sarcini în numele lor – acest lucru se face prin emiterea unui mandat către reprezentant. Reprezentantul autorizat este obligat să furnizeze o copie a acestui mandat autorităților de supraveghere a pieței, dacă i se solicită acest lucru.

Atunci când producătorul alege să procedeze astfel, mandatul trebuie să permită reprezentantului autorizat să îndeplinească cel puțin următoarele sarcini:

- să păstreze declarația de conformitate UE și documentația tehnică (a se vedea secțiunea 4 din prezentele orientări) la dispoziția autorităților de supraveghere a pieței timp de cel puțin 10 ani după introducerea PDE pe piață sau pe durata perioadei de asistență, oricare dintre acestea este mai lungă;
- La cerere, să furnizeze autorităților de supraveghere a pieței toate informațiile și documentația necesare pentru a demonstra conformitatea PDE;
- Să coopereze cu autoritățile de supraveghere a pieței.

3.6 Organisme de evaluare a conformității

IMM-urile ar putea, de asemenea, să își asume rolul de organisme de evaluare a conformității (CAB), denumite și organisme notificate în CRA. Acestea sunt organizații independente desemnate de statele membre ale UE și notificate Comisiei Europene pentru a efectua evaluări de conformitate de către terți. Ele evaluează dacă anumite

produse digitale respectă cerințele de securitate cibernetică înainte de a se putea solicita marcajul CE.

CAB sunt responsabile în primul rând de efectuarea evaluărilor de conformitate în conformitate cu cerințele CRA (modulele B, C și H) și de verificarea documentației tehnice corespunzătoare. În cazul unei evaluări reușite, organismul notificat emite o declarație de conformitate, care este necesară pentru a obține marcajul CE.

În consecință, organismele de evaluare a conformității trebuie să fie:

- Acreditate și desemnate în conformitate cu normele UE[13]
- Competente din punct de vedere tehnic în domeniul securității cibernetice și al evaluării produselor

Acestea sunt supuse supravegherii naționale și coordonării la nivelul UE.

[13] Sistemul de informații NANDO (Organizații notificate și desemnate în conformitate cu noua abordare) https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies

4. Cerințe esențiale de securitate cibernetică

4.1 Referitoare la proprietățile produselor

4.1.1 Principiile „Securitate prin proiectare” și „Securitate implicită”

Cerințele CRA de adoptare a principiului securității prin proiectare și securității implicite, cu referire la acesta în mai multe puncte din text:

- Considerentul 32 din CRA recunoaște că *„protecția datelor încă din faza de proiectare și în mod implicit, precum și securitatea cibernetică în general, sunt elemente cheie ale Regulamentului (UE)* 2016/679”[14] .
- Considerentul 34 prevede că *„Atunci când integrează componente provenite de la terți în produse cu elemente digitale în faza de proiectare și dezvoltare, producătorii ar trebui, pentru a se asigura că produsele sunt proiectate, dezvoltate și fabricate în conformitate cu cerințele esențiale de securitate cibernetică prevăzute în prezentul regulament”*,
- Articolul 13 alineatul (1), care detaliază obligațiile producătorilor, prevede că *„Atunci când introduc pe piață un produs cu elemente digitale, producătorii se asigură că acesta a fost proiectat, dezvoltat și produs în conformitate cu cerințele esențiale de securitate cibernetică prevăzute în partea I din anexa I*.”
- Anexa I, care detaliază cerințele esențiale de securitate cibernetică, prevede că *„(1) Produsele cu elemente digitale trebuie proiectate, dezvoltate și fabricate astfel încât să asigure un nivel adecvat de securitate cibernetică în funcție de riscuri.”*

Ca dovadă a respectării principiului securității prin proiectare, IMM-urile pot utiliza planul de gestionare a riscurilor pentru dezvoltarea produselor, inclusiv identificarea riscurilor, analiza și strategiile de atenuare a riscurilor pentru fiecare etapă de dezvoltare.

14Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (Text cu relevanță pentru SEE)

Mai explicit, anexa I punctul (2) litera (b) prevede o cerință explicită pentru o configurație implicită sigură: *„Produsele cu elemente digitale: (b) sunt puse la dispoziție pe piață cu o configurație implicită sigură, cu excepția cazului în care producătorul și utilizatorul comercial au convenit altfel în legătură cu un produs personalizat cu elemente digitale, inclusiv posibilitatea de a reseta produsul la starea sa inițială."*

Aceste concepte nu sunt definite în text, iar semnificația lor se presupune a fi evidentă. De exemplu, autoritatea de reglementare germană – Oficiul Federal pentru Securitatea Informațiilor din Germania (BSI)[15] – completează explicând că principiul CRA „securitate prin proiectare" înseamnă că *„produsele conectate trebuie proiectate ținând seama de securitatea cibernetică, de exemplu prin asigurarea faptului că datele stocate sau transmise cu produsul sunt criptate și că suprafața de atac este cât mai mică posibil"*, iar pentru principiul „securitate implicită", *„setările implicite ale produselor conectate în rețea trebuie să contribuie la creșterea securității acestora, de exemplu prin interzicerea parolelor implicite slabe, prin instalarea automată a actualizărilor de securitate etc."*

În ceea ce privește dovezile acceptabile pentru conformitatea cu principiul securității implicite, IMM-urile ar trebui să ia în considerare documentarea regulilor de configurare securizată aplicate și, în cazul în care produsul este personalizat, să ofere un acord adecvat cu utilizatorii săi comerciali, cu clauze relevante.

În practică, interpretarea acestor cerințe trebuie să se bazeze pe evaluarea riscurilor și va fi la latitudinea producătorului, reflectând natura produsului și contextul în care acesta va fi utilizat.

4.1.2 Gestionarea riscurilor de securitate cibernetică

Evaluarea riscurilor de securitate cibernetică stă la baza întregii abordări a securității cibernetice prevăzute în CRA, promovând o abordare proactivă a gestionării riscurilor care justifică măsurile de securitate cibernetică, în opoziție cu o abordare de conformitate[16] . Evaluarea riscurilor este o piatră de temelie a securității produselor, oferind o modalitate sistematică de identificare, evaluare și prioritizare a potențialelor amenințări încă din primele etape de dezvoltare și pe tot parcursul ciclului de viață al produsului. Prin actualizarea continuă a evaluării riscurilor pe măsură ce produsul evoluează, organizațiile se asigură că măsurile de securitate rămân solide și relevante, protejând în mod eficient atât produsul, cât și utilizatorii acestuia. Acest proces nu numai

[15] BSI - Oficiul Federal pentru Securitatea Informațiilor din Germania (2025) Regulamentul UE privind reziliența cibernetică, disponibilă la: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html#:~:text=Take%20cybersecurity%20into%20account,not%20have%20to%20be%20published.. accesat la 21 iulie 2025

[16] Referirea la gestionarea riscurilor se face și în considerentele 37, 38, 39, 48 și 52 (referitoare la evaluarea coordonată la nivelul Uniunii a riscurilor de securitate ale lanțurilor de aprovizionare critice), 53, 55, 58, 114

că ghidează selecția și rigurozitatea controalelor de securitate, dar servește și ca bază pentru toate evaluările și deciziile ulterioare în materie de securitate. Respectarea bunelor practici stabilite - precum cele descrise în ISO 31000 sau ISO 14971 - asigură o abordare cuprinzătoare și repetabilă. În cele din urmă, evaluarea riscurilor nu este doar esențială pentru crearea de produse sigure, ci este și o condiție prealabilă obligatorie pentru conformitatea cu CRA și orice altă reglementare UE în materie de securitate cibernetică sau siguranță. Într-adevăr, CRA în sine utilizează tehnici de evaluare a riscurilor pentru a defini o serie de clase de produse și pentru a stabili cerințe de securitate care să reflecte nivelul de risc asociat fiecărei clase de produse. Un model de evaluare a riscurilor este disponibil în anexa B la prezentul document.

Mai mult, evaluarea riscurilor pentru PDE în conformitate cu CRA este o evaluare specifică produsului, care depășește evaluările de risc individuale ale proiectului sau ale organizației. Pentru a îndeplini cerințele CRA, evaluarea trebuie să abordeze în mod specific securitatea:

- **utilizatorilor finali**, adică informațiile și instrucțiunile care trebuie furnizate utilizatorului,
- **evaluarea riscurilor lanțului de aprovizionare**, inclusiv vulnerabilitățile identificate prin intermediul listei de componente software (SBOM), inclusiv prin elaborarea unei liste de componente software într-un format utilizat în mod obișnuit și lizibil de mașini, care să acopere cel puțin dependențele de nivel superior ale produselor și să ia în considerare SBOM în cerințele de gestionare a vulnerabilităților discutate mai jos, și
- **luarea în considerare a modului în care PDE sau dispozitivele sale conectate ar putea afecta alte** rețele și produse cu care interacționează, adică cerințele de proiectare a produsului discutate mai jos.

Această perspectivă cuprinzătoare asigură că nu numai produsul în sine, ci și ecosistemul și utilizatorii acestuia sunt protejați de amenințările în continuă evoluție și că măsurile de securitate sunt adaptate riscurilor interconectate din lumea reală.

Referințele cheie din textul CRA sunt:

- ➔ Articolul 3 alineatele (37) și (38) definesc conceptele de „risc de securitate cibernetică” și, respectiv, „risc semnificativ de securitate cibernetică”.
- ➔ Articolul 13 prevede cerințe explicite privind modul în care producătorii ar trebui să gestioneze riscurile pentru a asigura un nivel adecvat de securitate pentru produsele lor, alineatul (13) alineatul (3) enumerând componentele pe care trebuie să le includă, cel puțin, cum ar fi analiza riscurilor bazată pe scopul prevăzut al PDE și utilizarea previzibilă în mod rezonabil, condițiile de utilizare, cum ar fi mediul operațional sau activele care trebuie protejate și altele.

➔ Anexa I (punctul 2) stabilește o serie de cerințe esențiale în materie de securitate cibernetică *pe baza evaluării riscurilor de securitate cibernetică menționate la articolul 13 alineatul (2).*

4.1.3 Obiectivele de securitate

Securitatea produselor este un element fundamental al Regulamentului UE privind reziliența cibernetică (CRA), care impune organizațiilor să integreze măsuri de securitate solide pe parcursul întregului ciclu de viață al produsului, de la proiectare și dezvoltare până la implementare și întreținere. Domeniile cheie includ:

- **Gestionarea identității și a accesului**: asigurarea faptului că numai utilizatorii și sistemele autorizate pot accesa funcții și date sensibile, reducând riscul de acces neautorizat și utilizare abuzivă;
- **Jurnalizare**: implementarea unei jurnalizări cuprinzătoare pentru a monitoriza activitatea, a detecta anomalii și a sprijini investigațiile criminalistice în caz de incidente;
- **Securitatea și minimizarea datelor**: protejarea datelor în fiecare etapă și colectarea numai a ceea ce este strict necesar, ceea ce limitează expunerea și reduce riscurile de conformitate;
- **Backup și ștergere sigură**: efectuarea de backup-uri regulate ale datelor critice și asigurarea ștergerii sigure a datelor atunci când acestea nu mai sunt necesare, prevenind pierderea datelor și recuperarea neautorizată;
- **Criptare**: protejarea informațiilor în tranzit și în repaus, făcând datele ilizibile pentru părțile neautorizate, menținând astfel confidențialitatea.

Prin integrarea acestor controale pe parcursul ciclului de viață al produsului, organizațiile pot îndeplini cerințele CRA, pot spori încrederea și pot proteja utilizatorii împotriva amenințărilor cibernetice în continuă evoluție și emergente.

Anexa I la CRA, la punctul (2), enumeră obiectivele specifice de securitate care trebuie implementate de producător, dar clarifică faptul că detaliile privind modul de implementare a acestor mecanisme vor reflecta evaluarea riscurilor efectuată pentru produs. Aceste mecanisme de control includ practici, proceduri și măsuri tehnice - cele mai importante mecanisme sunt discutate pe scurt mai jos.

Cerințe privind proiectarea produsului
Produsele trebuie:
(j) să fie proiectate, dezvoltate și produse astfel încât să limiteze suprafețele de atac, inclusiv interfețele externe;
(k) să fie proiectate, dezvoltate și produse astfel încât să reducă impactul unui incident utilizând mecanisme și tehnici adecvate de atenuare a exploatării

Aceste cerințe de proiectare trebuie luate împreună cu cerința de configurare securizată în mod implicit.

Ca dovadă a conformității cu cerințele de mai sus, IMM-urile trebuie să încorporeze, să implementeze și să monitorizeze evaluări cuprinzătoare ale riscurilor produselor, să coreleze riscurile cu serviciile și controalele, să evalueze documentația de proiectare, să revizuiască codul, să asigure medii separate de producție și dezvoltare, să stabilească și să monitorizeze nivelurile de referință de securitate pentru a identifica anomaliile și să impună efectuarea de copii de rezervă periodice ale software-ului și datelor.

Măsuri de detectare și eliminare a vulnerabilităților pe parcursul ciclului de viață al produsului

Detectarea și eliminarea vulnerabilităților înainte de lansarea software-ului este o cerință esențială a CRA

Produsele cu elemente digitale trebuie:

(a) să fie puse la dispoziție pe piață fără vulnerabilități exploatabile cunoscute;

Vulnerabilitățile cunoscute sunt enumerate în bazele de date publice privind vulnerabilitățile, de exemplu în baza de date a UE privind vulnerabilitățile[17] sau în baza de date națională a SUA privind vulnerabilitățile[18] sau în instrumentele de scanare a vulnerabilităților (a se vedea metodologia de testare penetrantă Confirmate pentru mai multe detalii privind scanarea și gestionarea vulnerabilităților).

Atunci când se constată că o vulnerabilitate a fost deja exploatată pentru un atac cibernetic, producătorul trebuie să ia măsurile necesare pentru a împiedica exploatarea cu succes a acesteia împotriva PDE înainte și după introducerea pe piață. Mulți hackeri, chiar și cei fără competențe avansate, profită de vulnerabilitățile cunoscute, dar necorectate, prin exploatări de tip „zero-day”.

(c) să se asigure că vulnerabilitățile pot fi remediate prin actualizări de securitate, inclusiv, după caz, prin actualizări automate de securitate care sunt instalate într-un interval de timp adecvat, activate ca setare implicită, cu un mecanism de renunțare clar și ușor de utilizat, prin notificarea utilizatorilor cu privire la actualizările disponibile și opțiunea de a le amâna temporar;

A doua parte a cerințelor esențiale de securitate este dedicată în întregime gestionării vulnerabilităților.

Odată identificată o vulnerabilitate, este important ca aceasta să fie evaluată în funcție de gravitate, conform unui cadru acceptat, cum ar fi CVSS (Common Vulnerability

[17] Disponibil la: https://euvd.enisa.europa.eu/
[18] Disponibil la: https://nvd.nist.gov/

Scoring System). Prioritizarea se face în funcție de acest scor, astfel încât vulnerabilitățile critice și exploatate în mod activ să fie remediate cu urgență. Remedierea se realizează, de obicei, prin lansarea unui patch sau a unei modificări de configurare.

În conformitate cu CRA, producătorii au obligația clară de a transmite aceste actualizări de securitate utilizatorilor fără întârzieri nejustificate, utilizând mecanisme de actualizare sigure și de a face acest lucru separat de actualizările de funcții. Actualizările trebuie furnizate gratuit, însoțite de mesaje de avertizare clare și, acolo unde este posibil, activate pentru instalare automată în mod implicit. Acest lucru asigură protecția promptă a utilizatorilor, chiar dacă aceștia nu acționează în mod proactiv. Cele mai bune practici din industrie recomandă acorduri privind nivelul de servicii (SLA) pentru gestionarea patch-urilor. De exemplu:

- 24 până la 48 de ore pentru remedierea vulnerabilităților critice
- 7 zile pentru vulnerabilități ridicate
- 30 de zile pentru vulnerabilități medii
- 90 de zile pentru vulnerabilități reduse

După remediere, monitorizarea continuă este esențială. Producătorii trebuie să se asigure că patch-urile au fost aplicate în mod eficient și să monitorizeze orice încercări de exploatare a vulnerabilităților rămase, inclusiv prin analizarea jurnalelor de sistem și acordarea atenției alertelor de detectare a intruziunilor.

Capcane de evitat:

- Amânarea remediilor până la actualizarea funcționalităților
- Subestimarea gravității vulnerabilităților
- Neinformarea utilizatorilor în timp util și într-un mod ușor de înțeles.

În plus, aplicarea în grabă a patch-urilor fără testarea corespunzătoare poate introduce noi probleme sau riscuri. Prin urmare, combinând remedierea promptă, implementarea patch-urilor și monitorizarea continuă, IMM-urile pot stabili un proces solid de gestionare a vulnerabilităților care să îndeplinească cerințele esențiale de securitate cibernetică ale CRA.

Dovezile recomandate pentru a demonstra conformitatea cu cerințele de mai sus, pe lângă elaborarea și aplicarea politicilor și procedurilor relevante, ar putea include teste de penetrare (interne și efectuate de terți), mecanisme automate de actualizare a securității, revizuiri ale codului și, cel mai important, actualizări relevante (chiar proactive) în timp util, în cazul în care se constată o nouă amenințare sau vulnerabilitate, chiar dacă aceasta nu a fost încă exploatată.

Cerințe tehnice

Exemple de măsuri tipice pentru îndeplinirea cerințelor tehnice ale CRA sunt enumerate în toate standardele de securitate a informațiilor, inclusiv NIST SP800 sau Cyber Fundamentals (CyFun) în secțiunea respectivă: Protejare. Exemple de măsuri specifice sunt prezentate mai jos.

(d) asigurarea protecției împotriva accesului neautorizat prin mecanisme de control adecvate, inclusiv, dar fără a se limita la, sisteme de autentificare, de gestionare a identității sau a accesului, și raportarea accesului neautorizat posibil;

Măsurile relevante recomandate de Cadrul NIST pentru securitatea cibernetică includ:

- Solicitarea autentificării multifactoriale;
- Aplicarea politicilor privind puterea minimă a parolelor, codurilor PIN și a altor mijloace de autentificare similare;
- Reautentificarea periodică a utilizatorilor, serviciilor și hardware-ului în funcție de risc (de exemplu, în arhitecturi zero trust);
- Asigurarea faptului că personalul autorizat poate accesa conturile esențiale pentru protejarea siguranței în condiții de urgență.

(e) protejarea confidențialității datelor stocate, transmise sau prelucrate în alt mod, personale sau de altă natură, de exemplu prin criptarea datelor relevante stocate sau în tranzit cu ajutorul unor mecanisme de ultimă generație și prin utilizarea altor mijloace tehnice;

Orientările relevante privind fundamentele cibernetice ca măsuri includ:

- Luați în considerare utilizarea tehnicilor de criptare pentru stocarea, transmiterea sau transportul datelor (de exemplu, laptop, USB);
- Mecanismele de verificare a integrității de ultimă generație (de exemplu, verificări de paritate, verificări de redundanță ciclică, hash-uri criptografice) și instrumentele asociate pot monitoriza automat integritatea sistemelor informatice și a aplicațiilor găzduite.

Orientări similare pot fi găsite și în alte standarde relevante:

(f) protejarea integrității datelor stocate, transmise sau prelucrate în alt mod, personale sau de altă natură, a comenzilor, programelor și configurațiilor împotriva oricărei manipulări sau modificări neautorizate de utilizator și raportarea corupțiilor;

(g) să prelucreze numai date, personale sau de altă natură, care sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopul prevăzut al produsului cu elemente digitale (minimizarea datelor);

(h) protejarea disponibilității funcțiilor esențiale și de bază, inclusiv după un incident, printre altele prin măsuri de reziliență și de atenuare împotriva atacurilor de tip „denial-of-service”;

Este important de menționat că CRA identifică CE trebuie făcut, dar nu CUM trebuie făcut. Modul în care aceste cerințe sunt puse în aplicare este la latitudinea producătorului, deși există o așteptare clară ca metodele adoptate să fie proporționale cu nivelul de risc asociat produsului.

IMM-urile ar putea demonstra conformitatea cu cerințele de mai sus prin dotarea produselor lor cu elemente digitale cu funcționalități de jurnalizare care să le permită integrarea în mediul de securitate cibernetică al utilizatorilor lor comerciali. Integrarea ar trebui să ia în considerare și compatibilitatea cu controlul centralizat al accesului, testat periodic, inclusiv prin teste de penetrare, și, nu în ultimul rând, criptografia avansată.

Măsurile de securitate specifice pe care IMM-urile trebuie să le ia în considerare, cel puțin, pentru a satisface cerințele de mai sus, includ:

- Adoptarea de politici și proceduri privind identitatea, controlul accesului, autorizarea și gestionarea incidentelor.
- Implementarea de măsuri de protecție dedicate pentru a preveni accesul neautorizat, denaturarea sau modificarea datelor de sistem și a înregistrărilor de audit (de exemplu, drepturi de acces restricționate, copii de rezervă zilnice, criptarea datelor, instalarea unui firewall).
- Implementarea mecanismelor de detectare și raportare a integrității.
- Activarea autentificării multifactoriale.
- Aplicarea politicilor privind puterea minimă a parolelor, codurilor PIN și a altor mijloace de autentificare similare.
- Implementați mecanisme de detectare și răspuns la atacuri DDoS.

<u>Măsuri pentru minimizarea impactului asupra mediului IT</u>
Există două cerințe care vizează minimizarea impactului unui incident sau al unei defecțiuni a produsului asupra mediului său, și anume punctele (i) și (k) descrise mai jos:
(i) minimizarea impactului negativ al produselor în sine sau al dispozitivelor conectate asupra disponibilității serviciilor furnizate de alte dispozitive sau rețele;

Această cerință impune ca PDE-urile să fie nu numai sigure pentru contul lor, ci și să nu reprezinte o amenințare pentru disponibilitatea altor dispozitive sau rețele. Este similară cu Directiva privind echipamentele radio, în care dispozitivele nu trebuie să „interfereze cu alte dispozitive sau rețele”, impunând echipamentelor să utilizeze în mod eficient spectrul radio și să respecte standardele de compatibilitate electromagnetică, prevenind

interferențele dăunătoare. Aplicată în domeniul securității cibernetice, am putea recomanda ca PDE-urile să fie proiectate cu atenție pentru a evita consumul excesiv de date, CPU sau rețea, de exemplu, și să aibă puncte de control pentru a evita utilizarea lor în atacuri de tip „denial of service". Într-un atac de tip „denial of service", PDE-urile compromise ar putea intra într-o armată de roboți (dispozitive compromise), atacând simultan o rețea, un site web sau o aplicație, blocând produsul sau rețeaua atacată.

(k) să fie proiectate, dezvoltate și produse astfel încât să reducă impactul unui incident utilizând mecanisme și tehnici adecvate de atenuare a exploatării;

Măsurile de securitate specifice pe care IMM-urile trebuie să le ia în considerare, cel puțin, pentru a satisface cerințele de mai sus, includ:

- Efectuarea unei evaluări cuprinzătoare a riscurilor produsului încă din faza de concepție, inclusiv luarea în considerare a riscurilor potențiale privind disponibilitatea serviciilor furnizate de alte dispozitive sau rețele din cauza PDE sau a dispozitivelor conectate și identificarea măsurilor de atenuare pentru a reduce impactul sau probabilitatea riscului.
- Implementarea de măsuri de protecție dedicate pentru a preveni accesul neautorizat, distorsionarea sau modificarea datelor sistemului și a înregistrărilor de audit (de exemplu, drepturi de acces restricționate, copii de rezervă zilnice, criptarea datelor, instalarea unui firewall).
- Implementarea mecanismelor de detectare și răspuns la DDoS.

Controale legate de utilizatori

Două măsuri suplimentare vizează capacitarea utilizatorului de a-și gestiona propria securitate și date:

(l) furnizarea de informații legate de securitate prin înregistrarea și monitorizarea activităților interne relevante, inclusiv accesul la sau modificarea datelor, serviciilor sau funcțiilor, cu un mecanism de renunțare pentru utilizator;

Tehnicile de detectare a comportamentului anormal care indică un atac cibernetic se bazează în principal pe revizuirea și analizarea jurnalelor produselor cu elemente digitale, pentru a determina tipul și vectorul atacului și a lua măsurile adecvate de răspuns. Acest lucru se realizează de obicei cu instrumente automatizate de colectare și corelare a jurnalelor, pentru care produsele cu elemente digitale trebuie să aibă funcționalitatea necesară pentru înregistrarea și monitorizarea activităților lor.

(m) să ofere utilizatorilor posibilitatea de a șterge în mod permanent, în condiții de siguranță și cu ușurință, toate datele și setările și, în cazul în care aceste date pot fi

transferate către alte produse sau sisteme, să se asigure că acest lucru se face în condiții de siguranță.

Tehnicile de eliminare sigură a datelor sunt diverse, în funcție de tipul suportului (hârtie, unitate de stocare, cloud) sau de nivelul de sensibilitate (de la date generice la istoricul clienților).

Măsurile de securitate specifice pe care IMM-urile trebuie să le ia în considerare, cel puțin, pentru a satisface cerințele de mai sus, includ:

- Integrarea funcționalității de sprijin pentru înregistrarea și monitorizarea activităților PDE.
- Integrarea funcționalităților de ștergere și transfer securizat al datelor și oferirea posibilității utilizatorului de a lansa procesul într-un mod simplu.
- Utilizarea unor metode precum suprascrierea completă a memoriei, ștergerea bazată pe criptare, umplerea cu zerouri, ștergerea la nivel de hardware sau chiar distrugerea fizică pentru a se asigura că datele sunt cu adevărat irecuperabile. Este esențial să se identifice toate secretele stocate înainte de ștergere, să se valideze că datele au dispărut și să se revocă certificatele dispozitivelor în timpul procesului.

CRA presupune că hackerii pot obține informații importante (sau chiar confidențiale) pentru planificarea atacurilor lor, pe care le pot extrage din PDE la care au acces după ce acestea sunt scoase din uz sau înlocuite cu altele, cu excepția cazului în care există un mecanism sigur pentru distrugerea în siguranță a datelor vechi și curățarea spațiului de stocare abandonat.

4.2 Lanțurile de aprovizionare și securitatea terților

Producătorii sunt responsabili pentru securitatea cibernetică a întregului produs pe care îl fabrică, inclusiv a oricăror componente terțe încorporate sau integrate, cum ar fi bibliotecile software, modulele open-source și firmware-ul. În special, producătorii trebuie să evalueze și să gestioneze riscurile provenite din lanțul de aprovizionare și trebuie să verifice dacă software-ul terț respectă cerințele CRA.

În practică, acest lucru înseamnă că orice responsabilitate impusă producătorului trebuie să fie asumată și de lanțul de aprovizionare corespunzător, dacă aceasta are un impact asupra produsului final. Exemple de așteptări includ, dar nu se limitează la:

- Securitate prin proiectare și implicit;
- Prelungirea perioadei de asistență (trebuie să fie compatibilă cu cea a produsului final);
- Gestionarea și divulgarea vulnerabilităților;

- Gestionarea incidentelor (în măsura în care există un impact asupra produsului producătorului).

În consecință, producătorii vor trebui să exercite diligența necesară în selectarea furnizorilor și a altor terți care contribuie la produsele lor.

Ca parte a acestei activități, producătorii trebuie să mențină și să furnizeze o listă de componente software (SBOM), care să enumere toate componentele software utilizate, inclusiv dependențele de terți și de surse deschise. SBOM trebuie să fie:

- Disponibilă într-un format lizibil de către mașini, la cererea clienților și a autorităților de supraveghere a pieței;
- Actualizată și să reflecte toate modificările pe parcursul ciclului de viață al produsului.

Detalii suplimentare privind formatul (de exemplu, JSON) și elementele (informațiile) SBOM pot fi furnizate de Comisia Europeană sub forma unui act de punere în aplicare.

În paralel, Agenția pentru Securitate Cibernetică și Infrastructură (CISA) din SUA oferă o perspectivă asupra celor mai bune practici și cerințelor minime în proiectul său din august 2025 intitulat „Elemente minime pentru o listă de componente software (SBOM)".

Pentru IMM-urile care fabrică produse acoperite de CRA, aceste cerințe SBOM în evoluție ale CISA clarifică aspectele tehnice și standardele pentru întreținerea SBOM. Însă detaliile CISA introduc și o complexitate operațională deloc neglijabilă.

4.3 Gestionarea vulnerabilităților

Partea II a cerințelor esențiale de securitate (anexa I la CRA) se referă la cerințele privind gestionarea vulnerabilităților. Există o oarecare suprapunere cu cerințele din partea I (de exemplu, cerința ca produsele cu elemente digitale să fie puse la dispoziție pe piață fără vulnerabilități exploatabile cunoscute). Cu toate acestea, majoritatea cerințelor enumerate în această parte a anexei sunt orientate către politici și proceduri și vizează în mod explicit gestionarea vulnerabilităților.

4.3.1 Identificare și documentare

(1) identificarea și documentarea vulnerabilităților și a componentelor conținute în produsele cu elemente digitale, inclusiv prin întocmirea unei liste de materiale software într-un format utilizat în mod obișnuit și lizibil de mașini, care să acopere cel puțin dependențele de nivel superior ale produselor;

Cerința de a întocmi o listă de materiale software (SBOM) este obligatorie. Informații suplimentare privind modul în care conceptul de SBOM se raportează la CRA pot fi găsite în considerentele 77, 118 și articolul 13 alineatul (24) din CRA.

După cum s-a menționat mai sus, la momentul redactării prezentului document, nu există un format impus pentru un astfel de document și nici un format standard acceptat, deși articolul 13 alineatul (24) permite Comisiei, prin intermediul unor acte de punere în aplicare care țin seama de standardele și bunele practici europene sau internaționale, să specifice formatul și elementele SBOM.
În plus, producătorii trebuie *(3) să aplice teste și revizuiri eficiente și periodice ale securității produsului cu elemente digitale;*
Aici este important de menționat că cerința (3) este de a stabili un proces cuprinzător și periodic de testare și revizuire, atât pentru vulnerabilitățile tehnice și organizaționale, cât și pentru configurațiile incorecte, indiferent dacă a fost descoperită sau nu o vulnerabilitate.

4.3.2 Remediere

Vulnerabilitățile PDE trebuie remediate fără întârziere. Acest lucru este necesar pentru a se asigura că produsul rămâne sigur pe piața UE. În plus, CRA a specificat că, acolo unde este posibil, noile actualizări de securitate trebuie furnizate separat de actualizările de funcționalitate. Acest lucru ar putea contribui la remedierea diferenței de timp între dezvoltarea produsului și întreținerea securității.

4.3.3 Dezvăluirea vulnerabilităților și schimbul de informații

Există trei cerințe cheie în acest domeniu:
(4) odată ce o actualizare de securitate a fost pusă la dispoziție, să se partajeze și să se dezvăluie public informații despre vulnerabilitățile remediate, inclusiv o descriere a vulnerabilităților, informații care să permită utilizatorilor să identifice produsul cu elementele digitale afectate, impactul vulnerabilităților, gravitatea acestora și informații clare și accesibile care să ajute utilizatorii să remedieze vulnerabilitățile; în cazuri justificate în mod corespunzător, în care producătorii consideră că riscurile de securitate ale publicării depășesc beneficiile de securitate, aceștia pot amâna divulgarea publică a informațiilor privind o vulnerabilitate remediată până după ce utilizatorii au avut posibilitatea de a aplica patch-ul relevant;
(5) să pună în aplicare și să aplice o politică privind divulgarea coordonată a vulnerabilităților;
(6) să ia măsuri pentru a facilita schimbul de informații cu privire la potențialele vulnerabilități ale produsului lor cu elemente digitale, precum și ale componentelor terțe conținute în produsul respectiv, inclusiv prin furnizarea unei adrese de contact pentru raportarea vulnerabilităților descoperite în produsul cu elemente digitale;

Cerința (5) se referă la divulgarea coordonată a vulnerabilităților, care are o semnificație specifică în acest context. Ideea care stă la baza divulgării coordonate a vulnerabilităților

(CVD) este descrisă pe larg de ENISA[19] . În esență, CVD este un set de norme (de exemplu, o politică) publicat de un producător care permite experților externi în securitate cu intenții bune (care pot fi „hackeri etici" sau servicii de scanare a vulnerabilităților) să identifice potențialele vulnerabilități ale sistemelor sau produselor sale și prevede o procedură (formular, canal, contacte) pentru raportarea către producător a punctelor slabe identificate în materie de securitate. CVD definește de obicei sistemele care intră în domeniul de aplicare, în ce condiții poate fi efectuată identificarea (fără încălcarea legii, fără a se produce prejudicii, fără scurgeri de date).

4.3.4 Gestionarea actualizărilor de securitate

Cerințele finale din partea II se referă la gestionarea actualizărilor de securitate, asigurând că remedierea (actualizările de securitate) discutată mai sus este fezabilă prin *mecanisme de distribuire în siguranță a actualizărilor* pentru PDE.

În plus, actualizările de securitate trebuie să fie gratuite și să fie însoțite de mesaje de avertizare care să furnizeze utilizatorilor informații relevante, inclusiv cu privire la măsurile potențiale care trebuie luate. Toate acestea au ca obiectiv să permită utilizatorilor PDE să își mențină produsele în siguranță și să ia măsurile necesare de reducere a riscurilor, atunci când este necesar.

5. Evaluarea conformității

5.1 Proceduri de evaluare a conformității

Procedurile de evaluare a conformității adoptate de CRA se bazează pe NLF[20] și se învârt în jurul principiului risc ridicat = asigurare ridicată. Și anume, categoriile implicite (care nu sunt menționate în mod specific în regulament) sunt supuse procedurilor de autoevaluare, clasa importantă I se bazează pe standardul armonizat sau pe evaluarea de către terți, clasa importantă II și produsul critic sunt supuse evaluării și certificării de către terți în consecință. Cerințele specifice pentru fiecare categorie de produse sunt rezumate în tabelul următor. Descrierea detaliată a procedurilor de evaluare a conformității este disponibilă în capitolul „Procesul de conformitate CRA" din

[19] https://www.enisa.europa.eu/topics/vulnerability-disclosure

[20] NLF (Noul cadru legislativ) clarifică utilizarea marcajului CE și creează un set de măsuri care pot fi utilizate în legislația privind produsele. NLF cuprinde: Regulamentul (CE) nr. 765/2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței produselor, Decizia nr. 768/2008 privind un cadru comun pentru comercializarea produselor, care include dispoziții de referință care trebuie incluse în revizuirile legislației privind produsele. În fapt, acesta este un model pentru viitoarea legislație privind armonizarea produselor, Regulamentul (UE) 2019/1020 privind supravegherea pieței și conformitatea produselor. Pentru mai multe detalii, vă rugăm să consultați site-ul web al Comisiei Europene: https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en

în procesul de conformitate CRA. Cerințele sunt prevăzute la articolul 32 din regulament. Anexa VIII oferă o descriere detaliată a procedurilor de evaluare a conformității.

CRA recunoaște și se bazează pe procedurile de conformitate prezentate mai jos.

5.1.1 Standarde armonizate. Acestea sunt standarde europene recunoscute oficial care conferă prezumția de conformitate cu cerințele legale specifice din legislația UE. Acestea servesc drept baze prescriptive și verificabile pentru gestionarea riscurilor, dezvoltarea sigură și securitatea operațională.

Aceste standarde trebuie încă elaborate și recunoscute oficial pentru a prezuma conformitatea cu cerințele esențiale de securitate cibernetică. În februarie 2025, Comisia Europeană a însărcinat organismele europene de standardizare (CEN, CENELEC, ETSI) să elaboreze 41 de standarde: 15 orizontale, care se aplică în general tuturor PDE, și 25 verticale, care sunt adaptate tipurilor specifice de produse și claselor de risc. Standardele orizontale se referă la cerințele generale de securitate (tip A) și vulnerabilitate (tip B), în timp ce standardele verticale oferă îndrumări detaliate pentru produse specifice, de exemplu browsere, dispozitive IoT (tip C), influențând posibilitatea producătorilor de a se autoevalua sau de a solicita conformitatea unei terțe părți, cele mai sensibile standarde fiind elaborate în condiții restricționate. O listă completă a standardelor poate fi găsită pe site-ul web CEN/CENELEC[21] .

Planificarea pentru livrarea acestor standarde prevede livrarea standardelor de tip A și a standardelor de tip B pentru gestionarea vulnerabilităților până la 30.08.26, a tuturor standardelor de tip C până la 30.10.26 și a standardelor de tip B rămase până la 30.10.27.

În plus față de standardele armonizate care sprijină în mod direct conformitatea cu CRA, producătorii sunt încurajați să utilizeze standardele de vârf din industrie atunci când pun în aplicare cerințele CRA. Exemple notabile sunt enumerate în apendicele C.

5.1.2 Specificațiile comune (adoptate prin actul de punere în aplicare al CE) sunt orientări detaliate și practice ale Comisiei Europene menite să ajute producătorii să îndeplinească cerințe specifice în materie de securitate cibernetică, în absența unor standarde armonizate sau pentru domenii care nu sunt suficient abordate într-un standard armonizat publicat, servind ca opțiune de rezervă în astfel de cazuri.

[21] Disponibil la: https://www.cencenelec.eu/media/CEN-CENELEC/News/Newsletters/2025/m_606_work_programme_final.pdf

5.1.3 Certificate emise în cadrul unui sistem european de certificare a securității cibernetice.

Sistemul principal de certificare al UE care va sprijini conformitatea cu CRA este EUCC (Criteriile comune europene). EUCC este un sistem de certificare a securității cibernetice la nivel european, bazat pe voluntariat, care permite certificarea produselor TIC, cum ar fi componentele tehnologice (cipuri, carduri inteligente), hardware și software. Bazându-se pe cadrul de evaluare SOG-IS Common Criteria, existent de peste douăzeci de ani, acesta servește ca o continuare și extindere (de la 17 state membre ale UE în prezent la toate cele 27 care îl adoptă). Acesta propune două niveluri de asigurare bazate pe nivelul de risc asociat utilizării prevăzute a produsului, serviciului sau procesului, în termeni de probabilitate și impact al unui accident.

Comisia Europeană a centralizat toate documentele și orientările legate de EUCC[22] . Optarea pentru o certificare UE în domeniul securității cibernetice ca procedură de evaluare a conformității aduce avantajul prezumției de conformitate cu CRA, chiar și pentru categoriile cu risc ridicat, și sporește credibilitatea pieței și încrederea clienților.

Regulamentul UE privind securitatea cibernetică (UE 2019/881) stabilește un cadru comun pentru certificarea securității cibernetice în întreaga UE. În temeiul Regulamentului UE privind reziliența cibernetică (CRA), acest cadru devine deosebit de important pentru produsele care prezintă riscuri mai mari, cele clasificate ca **fiind importante de clasa II** sau **critice** în anexa VIII. Pentru aceste clase de produse, certificarea poate servi drept dovadă formală a îndeplinirii unor niveluri de asigurare „substanțiale” sau „ridicate”.

5.2 Proceduri minime necesare de evaluare a conformității

IMM-urile ar trebui să îndeplinească cel puțin procedurile minime necesare prevăzute în CRA pentru categoria lor de produse, astfel cum se explică în documentul Confirmate D3.1 – Arhitectura pentru evaluarea automatizată a conformității CRA[23] **SAU** orice altă procedură mai exigentă. Cu cât procedura de evaluare aleasă este mai exigentă, cu atât PDE pare mai sigur și mai de încredere pe piață, ceea ce ar putea constitui un avantaj competitiv semnificativ. De exemplu, dacă PDE se încadrează în categoria Implicit, atunci procedura minimă necesară este Modulul A, dar IMM-ul poate alege oricare dintre celelalte proceduri mai exigente de mai jos. Dacă un PDE se încadrează în clasa importantă I, atunci IMM-ul care îl produce ar putea să se autoevalueze în raport cu standardele armonizate pentru tipul său de produs, dacă acestea sunt disponibile, sau, dacă nu sunt disponibile, să aleagă următoarea procedură mai exigentă – modulul B+C sau modulul H. Dacă un PDE este inclus în clasa importantă II, atunci procedurile

[22] Disponibil aici: https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en
[23] Disponibil lahttps://confirmate-project.eu/materials/

minime necesare sunt două: „modulul B+C” sau modulul H, ambele necesitând evaluarea de către o terță parte.

Opțiunile de procedură pentru produse specifice sunt rezumate în tabelul de mai jos, fiecare bifă indicând o opțiune pentru categoria respectivă:

Tip / categorie de produs	Implicit	Clasa importantă I	Clasa importantă II	Critică
Autoevaluare (Modulul A – Control intern)	✅			
Autoevaluare în raport cu standardul armonizat al UE, specificații comune (Modulul A – Control intern)	✅	✅		
Evaluarea CAB a proiectării + Autoevaluarea producției (Modulul B+C)	✅	✅	✅	
Asigurarea completă a calității CAB (Modulul H)	✅	✅	✅	
Certificat UE de securitate cibernetică (CSA) la nivel „substanțial” sau „ridicat”	✅	✅	✅	✅

Se face o excepție pentru produsele open source: *„Producătorii de produse importante cu elemente digitale care se califică drept software liber și open source ar trebui să poată urma procedura de control intern bazată pe modulul A, cu condiția să pună la dispoziția publicului documentația tehnică”* (considerentul 91 din CRA).

5.3 Marcajul CE și documentația tehnică

5.3.1 Marcajul CE

Marcajul CE este definit în CRA ca: *„marcajul prin care un producător indică faptul că un produs cu elemente digitale și procesele puse în aplicare de producător sunt în conformitate cu cerințele esențiale de securitate cibernetică prevăzute în anexa I și în alte acte legislative de armonizare ale Uniunii care prevăd aplicarea acestuia”.*
În general, marcajul CE este necesar pentru a atesta faptul că un produs îndeplinește toate cerințele aplicabile ale UE în materie de securitate cibernetică și siguranță. În contextul CRA, marcajul CE ar trebui aplicat numai după (a) finalizarea procedurii

relevante de evaluare a conformității și (b) redactarea și semnarea declarației de conformitate UE.
Marcajul CE este supus principiilor generale prevăzute la articolul 30 din Regulamentul (CE) nr. 765/2008. Marcajul CE trebuie să fie aplicat în mod vizibil, lizibil și indelebil pe produs și pe ambalaj sau pe documentația însoțitoare (dacă marcarea fizică nu este posibilă).

Notă importantă: *Nu toate produsele trebuie să aibă marcajul CE. Acesta este obligatoriu numai pentru majoritatea produselor care fac obiectul directivelor de nouă abordare. Este interzisă aplicarea marcajului CE pe alte produse. Vă rugăm să rețineți că marcajul CE nu indică faptul că un produs a fost aprobat ca fiind sigur de către UE sau de către o altă autoritate. De asemenea, acesta nu indică originea unui produs*[24] *.*

[24] *A se vedea textul integral și toate opțiunile de formatare a marcajului CE pe site-ul web al Comisiei Europene: https://single-market-economy.ec.europa.eu/single-market/goods/ce-marking_en*

5.3.2 Documentație tehnică

Producătorii sunt obligați să întocmească și să păstreze documentația tehnică (conform anexei VII la CRA), care demonstrează conformitatea produsului. Acest lucru este obligatoriu atât pentru autoevaluare, cât și pentru evaluarea de către terți.

Această documentație trebuie să includă:

- Descrierea generală a produsului
- O descriere a proiectării, dezvoltării și producției produsului
- Evaluări inițiale și actualizate ale riscurilor
- Informații relevante care au fost luate în considerare pentru a determina perioada de asistență
- O listă a standardelor armonizate aplicate integral sau parțial produsului
- Rapoarte de testare, rezultate ale inspecțiilor și standarde aplicate
- Descrierea procedurii de evaluare a conformității utilizate
- O copie a declarației de conformitate UE
- Dacă este cazul, lista componentelor software

Pentru IMM-uri, o opțiune pentru o formă simplificată a documentației tehnice va fi disponibilă într-un regulament de punere în aplicare al Comisiei care nu a fost încă publicat la momentul redactării prezentului ghid.

5.4 Declarația de conformitate

Declarația de conformitate (DoC) este un document legal care atestă că un produs îndeplinește cerințele esențiale aplicabile în materie de securitate cibernetică prevăzute în anexa I la CRA. Aceasta este întocmită de producător după finalizarea cu succes a procedurilor de evaluare a conformității corespunzătoare, trebuie semnată de un reprezentant autorizat și pusă la dispoziția autorităților naționale de supraveghere a pieței.

DoC trebuie să conțină:

- Numele și adresa producătorului
- Identificarea produsului
- O declarație de conformitate cu CRA
- O listă a standardelor relevante și a procedurilor de conformitate utilizate
- Referire la examinarea UE de tip (dacă este cazul)
- Semnătura, data și datele de contact ale persoanei responsabile

Conținutul declarației de conformitate este prezentat în anexele V și VI la CRA.

6. Obligații de raportare și post-comercializare

6.1 Obligații de raportare

În conformitate cu articolul 14, IMM-urile sunt obligate să raporteze atât „vulnerabilitățile exploatate activ", cât și „incidentele grave". Acestea sunt definite după cum urmează:

- O vulnerabilitate exploatată activ este o breșă de securitate deja utilizată sau care face obiectul unui atac malicios activ.
- Un incident grav este un eveniment care afectează confidențialitatea, integritatea și disponibilitatea produsului, inclusiv introducerea de programe malware.

Articolul 14 din CRA descrie în continuare un incident grav ca fiind un incident care (a) afectează negativ sau este capabil să afecteze negativ capacitatea unui PDE de a proteja disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor sau funcțiilor sensibile sau importante, SAU (b) a dus sau este capabil să ducă la introducerea sau executarea unui cod rău intenționat într-un PDE sau în rețeaua și sistemele informatice ale unui utilizator al produsului.
Cerințele de raportare pentru aceste două tipuri de evenimente diferă, după cum se explică în secțiunile următoare. Detalii pot fi găsite în articolul 14 din CRA.

Pe lângă raportarea obligatorie a oricărei vulnerabilități exploatate în mod activ și a oricărui incident grav, CRA presupune raportarea voluntară a oricărui alt incident sau amenințare la adresa PDE. Se aplică aceeași procedură de raportare simultană către CSIRT și ENISA prin intermediul platformei unice de raportare.

6.2 Procedura de raportare

Toate notificările obligatorii trebuie transmise prin intermediul viitoarei platforme unice de raportare[25] către ENISA și simultan către CSIRT-ul sediului principal al producătorului din UE. Odată ce platforma unică de raportare (a se vedea mai jos) va fi disponibilă, acest lucru se va realiza printr-o singură notificare către platformă.

Vulnerabilități exploatate activ

Raportarea vulnerabilităților exploatate în mod activ se realizează în trei etape distincte:

- Etapa 1: Avertizare timpurie în termen de **24 de ore** de la constatare. Dacă este cazul, statele membre în care produsul a fost pus la dispoziție ar trebui identificate în această etapă.
- Etapa 2: Raportul inițial privind vulnerabilitatea în termen de **72 de ore** de la constatare, incluzând:

[25] A se vedea articolul 16 din CRA: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847

- informații generale despre produs, natura exploatării și vulnerabilitatea în cauză.
- Orice măsuri corective sau de atenuare luate, precum și măsurile corective sau de atenuare pe care le pot lua utilizatorii.
- O evaluare de către producător a nivelului de sensibilitate al informațiilor notificate

- Etapa 3: Raport final în termen de cel mult **14 zile** de la disponibilitatea unei soluții, care include:
  - O descriere a vulnerabilității, inclusiv gravitatea și impactul acesteia;
  - Dacă sunt disponibile, informații privind orice actor rău intenționat care a exploatat sau exploatează vulnerabilitatea;
  - Detalii despre actualizarea de securitate sau alte măsuri corective care au fost puse la dispoziție pentru remedierea vulnerabilității.

Incidente grave de securitate

Raportarea incidentelor grave de securitate se realizează, de asemenea, în trei etape separate, diferența esențială fiind în etapa finală.

- Etapa 1: Avertizare timpurie în termen de **24 de ore** de la constatare, incluzând:
  - O opinie cu privire la faptul dacă incidentul este suspectat a fi cauzat de acte ilegale sau rău intenționate, care trebuie să indice, de asemenea.
  - Dacă este cazul, statele membre în care produsul a fost pus la dispoziție.
- Etapa 2: Raportarea incidentului în termen de **72 de ore** de la constatare, incluzând:
  - Natura incidentului
  - O evaluare inițială a incidentului
  - Orice măsuri corective sau de atenuare luate, precum și măsurile corective sau de atenuare pe care le pot lua utilizatorii
  - O evaluare de către producător a nivelului de sensibilitate al informațiilor notificate.
- Etapa 3: Raport final în termen de **o lună** de la notificarea în termen de 72 de ore, care include:
  - O descriere detaliată a incidentului, inclusiv gravitatea și impactul acestuia;
  - Tipul de amenințare sau cauza principală care ar fi putut declanșa incidentul;
  - Măsurile de atenuare aplicate și în curs de aplicare.

Notificarea utilizatorilor

Pentru ambele tipuri de incidente, odată ce au luat cunoștință de vulnerabilitate sau incident, producătorii trebuie să informeze fără întârziere utilizatorii afectați (și, după caz, toți utilizatorii), inclusiv sfaturi de atenuare a riscurilor într-un format ușor de automatizat

și lizibil de mașini. Dacă producătorii nu notifică, CSIRT poate interveni pentru a informa utilizatorii.

Raportarea voluntară

În afara obligațiilor de notificare, în conformitate cu articolul 15, producătorii sunt încurajați să raporteze în mod voluntar orice vulnerabilitate și amenințare care ar putea afecta securitatea cibernetică a unui PDE. Respectiv, notificarea incidentelor care nu sunt grave este, de asemenea, voluntară.

Acest mecanism de raportare voluntară ar putea introduce o bună practică pentru IMM-uri, cu un efect pozitiv indirect pentru producător și clienții săi, sporind vizibilitatea amenințării și, astfel, prevenind alte incidente. În plus, în cazul în care este dificil să se evalueze cu exactitate dacă o anumită vulnerabilitate este exploatată în mod activ sau dacă un incident este grav, raportarea voluntară pare a fi opțiunea sigură.

6.3 Cooperarea cu autoritățile UE și naționale

6.3.1 ENISA și CSIRT-urile privind gestionarea vulnerabilităților

Producătorii raportează vulnerabilitățile exploatate în mod activ și incidentele grave către ENISA și CSIRT național, în conformitate cu dispozițiile prevăzute la articolul 14 din actul legislativ. Cerințele impuse producătorului sunt prezentate în secțiunea 5.2 din prezentele orientări.

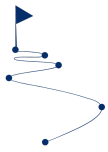
6.3.2 Autoritățile naționale de supraveghere a pieței

Autoritățile de supraveghere a pieței sunt responsabile de aplicarea obligațiilor CRA în fiecare județ. Modul în care acest lucru se aplică CRA este explicat în capitolul V din CRA.

Consecințele pentru producători sunt că aceștia sunt obligați să:

- Coopereze în timpul investigațiilor, auditurilor și inspecțiilor;
- Furnizeze documentația (de exemplu, SBOM, evaluări de risc, dosare tehnice) la cerere;

- Să informeze MSA cu privire la neconformități și măsuri corective, dacă este cazul.



7. Pașii pe care IMM-urile trebuie să îi urmeze pentru a implementa CRA

7.1 Evaluarea inițială a domeniului de aplicare și a lacunelor

Primul pas către conformitatea cu CRA este de a înțelege clar ce produse intră în domeniul de aplicare al CRA, care este rolul organizației în raport cu produsele din domeniul de aplicare și ce cerințe respectă și nu respectă produsele. Acest lucru se realizează prin efectuarea unei evaluări a domeniului de aplicare și a lacunelor.

Acest document, împreună cu instrumentele furnizate de proiectul CONFIRMATE, sunt menite să sprijine analiza inițială: domeniul de aplicare, identificarea rolului, evaluarea lacunelor și monitorizarea îmbunătățirilor în timp, pe măsură ce cerințele neconforme sunt abordate de organizație. În acest sens, evaluarea lacunelor ar trebui considerată un „document viu”, în sensul că ar trebui actualizată periodic pentru a reflecta progresele înregistrate. În acest fel, evaluarea va reflecta cu exactitate situația organizației în ceea ce privește conformitatea în orice moment.

7.2 Elaborarea unui plan de implementare

Planul de implementare poate fi elaborat după efectuarea evaluării inițiale a lacunelor. La fel ca evaluarea în sine, planul trebuie considerat un document care evoluează în timp și ține seama de lecțiile învățate pe măsură ce proiectul de implementare avansează.

În ceea ce privește planificarea, se recomandă adoptarea unei abordări „în valuri”, în care activitățile pentru următoarele trei luni sunt planificate la un nivel ridicat de detaliu, iar activitățile ulterioare sunt estimate pe baza eforturilor depuse. Introducerea prea multor detalii în planurile care se referă la un viitor îndepărtat poate fi contraproductivă, deoarece activitățile pe termen lung tind să fie modificate pentru a reflecta lecțiile învățate în fazele anterioare ale unui proiect.

În toate cazurile, dacă nu există deja, efectuarea unei evaluări a riscurilor ar trebui să fie o prioritate, deoarece rezultatele acestei evaluări vor justifica măsurile planificate și implementate și vor permite organizației să prioritizeze riscurile cât mai eficient posibil.

În ceea ce privește planificarea pe termen scurt, se recomandă ca activitățile să fie simple, să existe rezultate clare pentru fiecare sarcină și să se mențină durata alocată pentru fiecare activitate individuală cât mai scurtă posibil. Astfel se evită problema sarcinilor care sunt întotdeauna finalizate în proporție de 90 %, dar care par să nu ajungă niciodată la 100 %.

Nu în ultimul rând, IMM-urile pot profita pe deplin de resursele dezvoltate special pentru a le sprijini în conformarea cu CRA în cadrul Programului Europa digitală: instrumentele proiectului nostru CONFIRMATE, menționate în apendicele E, și alte proiecte, enumerate în apendicele F, precum și resursele de sprijin ale UE și naționale pentru IMM-uri enumerate în apendicele D.

7.3 Formarea și sensibilizarea personalului

Programele de formare și sensibilizare sunt o componentă cheie a planului de conformitate. Deși s-au depus toate eforturile pentru a simplifica cerințele CRA în aceste orientări și în instrumentele însoțitoare, este extrem de important ca personalul să dezvolte și să mențină o înțelegere aprofundată a CRA și a politicilor conexe.

În anexe sunt enumerate orientări suplimentare, instrumente și modele pe care IMM-urile le-ar putea utiliza pentru a pune în aplicare cerințele esențiale de securitate și pentru a se conforma cerințelor de documentare. Utilizarea acestor resurse nu este obligatorie, cu excepția modelului de declarație de conformitate, dar ar trebui luată în considerare în contextul unui plan la nivelul întregii organizații.

8. Termene și perioade de tranziție

Datele cheie din calendarul de punere în aplicare a CRA sunt următoarele:

Data	Eveniment
11.12.24	CRA intră în vigoare

11.06.26	Obligații de notificare a organismelor de evaluare a conformității aplicabile[26]
30.08.26	Termenul limită pentru standardele de tip A și standardele armonizate de tip B pentru gestionarea vulnerabilităților
11.09.26	Obligațiile de raportare a vulnerabilităților și incidentelor de securitate devin aplicabile.
30.10.27	Termenul limită pentru standardele armonizate de tip B rămase
11.12.27	Aplicarea integrală a CRA

Anexa A: Declarație simplificată de conformitate UE

Prin prezenta, ... [numele producătorului] declară că produsul cu elemente digitale de tip ... [denumirea tipului de produs cu element digital] este în conformitate cu Regulamentul (UE) 2024/2847 (1).

Textul integral al declarației de conformitate UE este disponibil la următoarea adresă de internet: ...

[26] Aceasta este o obligație a statelor membre, nu a producătorilor.

Anexa B: Model de evaluare a riscurilor

Setul de instrumente interoperabile ale ENISA pentru gestionarea riscurilor în UE oferă o metodologie armonizată și recunoscută la nivelul UE în acest scop. Acesta este conceput pentru a sprijini punerea în aplicare coerentă a gestionării riscurilor în întreaga UE, incorporând ISO/IEC 27005, NIS2 și practici specifice sectorului. Trebuie menționat însă că acest set de instrumente nu a fost conceput special pentru a îndeplini cerințele CRA, ci trebuie considerat un instrument cu scop general, care acoperă multe domenii de aplicare diferite.

Setul de instrumente include șabloane standardizate și orientări pentru:

- Identificarea și evaluarea activelor
- Analiza amenințărilor și vulnerabilităților
- Estimarea și evaluarea riscurilor
- Definirea măsurilor de tratare și atenuare a riscurilor
- Integrarea cu controalele de securitate prevăzute în anexa I la CRA[27]

Acesta acceptă atât evaluări calitative, cât și semicantitative și este interoperabil cu metodologiile naționale și internaționale. Utilizarea acestui set de instrumente permite consecvența, auditabilitatea și trasabilitatea completă a deciziilor de securitate în sprijinul evaluărilor de conformitate și al documentației tehnice în conformitate cu CRA.

[27] Rețineți că aceasta nu este o corespondență explicită cu controalele CRA.

Anexa C: Standarde relevante

- ETSI TS 103 701, anexele B și C pot fi utilizate pentru structurarea documentației tehnice pregătite pentru audit utilizând șabloanele ICS/IXIT
- **ISO/IEC 27001** - Sistemul de management al securității informației (ISMS)
- **ISO/IEC 27701** - Sistemul de management al informațiilor confidențiale (PIMS)
- ETSI EN 303 645 - Cerințe de securitate de bază pentru IoT de consum, unde clauzele 4-5 pot fi utilizate pentru definirea cerințelor de securitate de bază
- **OWASP ASVS** – Standard de verificare a securității aplicațiilor
- **CIS Benchmarks** - Ghiduri de configurare sigură
- **Linii directoare ale Fundației pentru securitatea IoT** – Cele mai bune practici în materie de securitate a dispozitivelor IoT
- **NIST SP 800-53** - **Controale de securitate și confidențialitate pentru sisteme informatice și organizații.**
- **NIST SP 800-37** - Cadru de gestionare a riscurilor (RMF), care oferă un proces care integrează activitățile de gestionare a riscurilor legate de securitate, confidențialitate și lanțul de aprovizionare cibernetic în ciclul de viață al dezvoltării sistemului.
- **Cadrul NIST pentru securitatea cibernetică (CSF)**, care oferă îndrumări privind gestionarea riscurilor de securitate cibernetică
- **IEC 62443 / ISA-62443** - Standarde de securitate pentru sistemele de automatizare și control industrial
- **ISO 9001** - Sistem de management al calității
- **CMMC** - Certificarea modelului de maturitate în domeniul securității cibernetice
- **GDPR** - Regulamentul general privind protecția datelor

Anexa D: Resurse de sprijin ale UE și naționale pentru IMM-uri

Comisia Europeană, Agenția UE pentru Securitate Cibernetică (ENISA) și Centrul European de Competență în Securitate Cibernetică (ECCC) publică rapoarte privind securitatea cibernetică, multe dintre acestea oferind orientări care ar putea fi utile IMM-urilor care implementează CRA.

În special, Ghidul pentru securizarea internetului obiectelor (IoT)[28] stabilește cerințele complete de securitate pe durata ciclului de viață, inclusiv cerințele și proiectarea, livrarea și întreținerea pentru utilizarea finală, precum și eliminarea. Studiul este elaborat special pentru a ajuta producătorii, dezvoltatorii, integratorii și toate părțile interesate implicate în lanțul de aprovizionare al IoT să ia decizii mai bune în materie de securitate atunci când construiesc, implementează sau evaluează tehnologiile IoT.

În plus, Ghidul ENISA privind securitatea cibernetică pentru IMM-uri este un ghid adaptat pentru îmbunătățirea securității cibernetice a organizațiilor mici, inclusiv a producătorilor.

La nivel național, misiunea centrelor naționale de competență în domeniul securității cibernetice este de a stimula excelența în cercetare și competitivitatea Uniunii în domeniul securității cibernetice. O listă a centrelor a fost publicată de Centrul european de competență în domeniul securității cibernetice (ECCC)[29] .

Pe lângă centrele de competență, multe state membre ale UE au creat o agenție națională de securitate cibernetică. În timp ce centrele de competență se concentrează pe cercetare și inovare, centrele de securitate cibernetică tind să acopere toate aspectele securității cibernetice (deși mandatele detaliate diferă de la un stat membru la altul). Exemple:

- **Belgia**: CCB - Centrul pentru securitate cibernetică din Belgia
- **Germania**: BSI – Oficiul Federal pentru Securitatea Informațiilor
- **Franța**: ANSSI – Agenția națională pentru securitatea sistemelor informatice
- **Italia**: ACN – Agenzia per la Cybersicurezza Nazionale
- **România**: DNSC – Directoratul Național de Securitate Cibernetică

Nu în ultimul rând, organizațiile industriale și profesionale creează resurse pentru a sprijini înțelegerea și respectarea CRA de către membrii lor. De exemplu, Alianța Digitală a IMM-urilor, ECSO (la nivel UE) și Agoria,

[28]Disponibil la: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things
[29]Disponibil la: https://cybersecurity-centre.europa.eu/nccs-0_en

Anexa E: Instrumente CONFIRMATE

Mai jos găsiți o scurtă prezentare generală a celorlalte ghiduri, cursuri de formare, instrumente și documente care însoțesc acest document. Toate materialele proiectului sunt disponibile pewww.confirmate-project.eu/materials .

Partea 1 Orientări și metodologii

Metodologia pentesting: document elaborat și revizuit de colegi, care are ca scop sprijinirea IMM-urilor în pregătirea și realizarea unui pentesting PDE eficient, aliniat la cerințele Regulamentului UE privind reziliența cibernetică (CRA). Bazat pe standardele industriei, acesta are ca scop sintetizarea și furnizarea unui ghid esențial cu privire la ceea ce este necesar și la ceea ce se poate aștepta ca rezultat al unui pentest al produsului, luând în considerare produse specifice, care se încadrează într-o serie de categorii CRA.

D3.1 - Arhitectura pentru evaluarea automatizată a conformității CRA: prezentare detaliată și cuprinzătoare a cadrului CONFIRMATE, care descrie în mod clar și metodic funcționalitatea și structura prevăzute. Documentul introduce și definește în mod clar procesul de evaluare a conformității, astfel cum este prevăzut de CRA, oferind cititorilor un context fundamental privind cerințele de reglementare. Ulterior, documentul ilustrează cu precizie modul în care utilizatorii finali vor interacționa cu cadrul CONFIRMATE și vor beneficia de acesta pe parcursul proceselor de evaluare a conformității CRA.
În urma descrierii orientate către utilizator, documentul specifică arhitectura software prevăzută, detaliind elemente esențiale precum componentele cheie, diviziunile modulare și interacțiunile dintre aceste elemente.

D2.2 - Modelul de date probatorii: o bază pentru colectarea și evaluarea automată a probelor tehnice din toate tehnologiile, asigurând captarea și organizarea eficientă a informațiilor necesare. Prin utilizarea formatelor lizibile de mașini, modelul facilitează integrarea probelor în instrumente automate de conformitate, reducând efortul manual necesar pentru documentare și îmbunătățind acuratețea evaluărilor de conformitate. Trebuie menționat însă că această abordare nu garantează conformitatea completă cu CRA, deoarece unele dintre cerințe nu pot fi transpuse în metode automate de colectare a datelor. Modelul de date probatorii permite și se aliniază la crearea de indicatori corespunzători, derivați din cerințele esențiale ale CRA. Acești indicatori oferă măsuri cuantificabile ale conformității.

Partea 2 Instrument automatizat open-source de evaluare a conformității

Confirmate propune un instrument de automatizare open-source care simplifică evaluarea conformității cu cerințele esențiale de securitate cibernetică CRA, enumerând toate cerințele și indicatorii esențiali de securitate cibernetică, comparând automat setările de securitate cu specificațiile CRA și determinând necesitățile individuale de acțiune. Tablourile de bord intuitive și capacitățile structurate ale acestuia ajută organizațiile să identifice rapid cerințele esențiale de securitate cibernetică CRA implementate și cele care trebuie evaluate sau implementate, economisind timp prețios în verificările de conformitate și oferind în același timp informații clare și utile pentru conformitate și îmbunătățire continuă.

În plus, instrumente de documentare precum:

- D2.2 – Modelul de date probatorii, care permit automatizarea verificării conformității printr-o abordare structurată a colectării și evaluării probelor.
- D3.1 – Arhitectura pentru evaluarea automată a conformității CRA, un document care oferă o prezentare detaliată și cuprinzătoare a cadrului CONFIRMATE, subliniind funcționalitatea și structura sa prevăzute, introducând procesul de evaluare a conformității și ilustrând modul în care utilizatorii finali vor interacționa cu CONFIRMATE și vor beneficia de acesta în procesul de evaluare a conformității CRA.

Partea 3 Cursuri și ateliere CONFIRMATE

Lista este un document în continuă actualizare, cu o serie de cursuri de formare și ateliere planificate până în iulie 2026.

Introducere în conformitatea CRA: Tot ce trebuie să știți despre Regulamentul UE privind reziliența cibernetică (CRA)[30] este o prezentare cuprinzătoare a principiilor și obligațiilor cheie ale CRA. Videoclipul explică modul în care CRA afectează producătorii, importatorii, distribuitorii și administratorii de software open-source, prezentând rolurile și responsabilitățile, clasificările produselor în funcție de risc (implicite, importante și critice), precum și cerințele de securitate, marcajul CE și evaluările de conformitate. De asemenea, acoperă subiecte cruciale, cum ar fi divulgarea vulnerabilităților, raportarea incidentelor, lista componentelor software (SBOM), termenele de aplicare și sancțiunile pentru neconformitate.

Metodologia pentesting explicată[31]

[30] Disponibil pe YouTubehttps://youtu.be/-QbPIFVobNw
[31] Disponibil pe YouTube: https://youtu.be/wpJluHL9IlQ

Ca parte a seriei de cursuri de formare privind conformitatea cu Regulamentul UE privind reziliența cibernetică (CRA), acest modul oferă un ghid cuprinzător, pas cu pas, privind metodologia testării de penetrare pentru produsele cu elemente digitale. Este conceput pentru producători, IMM-uri și echipe de securitate cibernetică care doresc să îndeplinească cerințele CRA în mod eficient și eficace. Formarea acoperă cele cinci etape cheie ale testării de penetrare aliniate la CRA și explică modul de planificare, desfășurare și raportare a testelor în conformitate cu standardele CRA. De asemenea, clarifică cerințele de conformitate pentru produsele din clasa importantă I, clasa importantă II și categoria implicită.

Anexa F: Alte instrumente ale proiectelor UE

Împreună cu CONFIRMATE, a fost lansat un set de proiecte suplimentare ale UE pentru a sprijini conformitatea IMM-urilor cu CRA. Fiecare proiect are o perspectivă diferită, provine dintr-un set diferit de țări și creează resurse și instrumente complementare. Lista proiectelor derulate în perioada 2025-2026, compilată de CyberStandEU[32] , este următoarea:

1. CRA-AI: Proiectul CRA-AI dezvoltă o platformă bazată pe inteligență artificială pentru a ajuta IMM-urile să atingă și să mențină conformitatea cu Regulamentul UE privind reziliența cibernetică, reunind experți în securitate cibernetică din șase țări ale UE.
2. CURIUM: CURIUM dezvoltă Compliance Continuum, un set de instrumente pentru automatizarea și simplificarea conformității cu Regulamentul UE privind reziliența cibernetică (CRA). Oferind evaluări de securitate cibernetică, gestionarea riscurilor și testarea vulnerabilităților, acesta ajută IMM-urile să reducă costurile, să accelereze certificarea și să consolideze ecosistemul de securitate digitală al Europei.
3. OSCRAT: OSCRAT dezvoltă instrumente gratuite, open-source, pentru a ajuta IMM-urile europene, factorii de decizie și asociațiile industriale să respecte Regulamentul UE privind reziliența cibernetică (CRA) și să consolideze practicile de securitate cibernetică.
4. OCCTET: OCCTET este un proiect finanțat de UE care dezvoltă un set de instrumente open-source pentru a ajuta IMM-urile să automatizeze conformitatea cu Regulamentul UE privind reziliența cibernetică (CRA) pentru software-ul open-source. Setul de instrumente include o listă de verificare a conformității, instrumente de evaluare automată, o bază de date federată, instrumente de analiză a dependențelor și resurse de raportare.
5. CYBERFORT: CYBERFORT ajută IMM-urile să îndeplinească cerințele Regulameentului UE privind reziliența cibernetică (CRA), oferind instrumente personalizate, îndrumare din partea experților și formare. Prin intermediul unei platforme deschise și al colaborării cu firme de securitate cibernetică, autorități și părți interesate din industrie, acesta consolidează reziliența cibernetică și conștientizarea în întreaga Europă.

[32] Disponibil la: https://cyberstand.eu/events/impacting-cra-defining-standards-future

6. TRUSTBOOST: TrustBoost este un proiect finanțat de UE (Acordul de grant nr. 101158687) susținut de Centrul european de competență în domeniul securității cibernetice. Misiunea sa este de a consolida securitatea cibernetică, reziliența și conformitatea în întreaga UE, prin promovarea colaborării în materie de certificare și respectarea legislației cheie a UE.
7. CRACoWi: CRACoWi (Cyber Resilience Act Compliance Wizard) este un proiect al UE care creează un asistent digital pentru a ajuta IMM-urile, producătorii, distribuitorii și importatorii să respecte standardele Regulamentului UE privind reziliența cibernetică (CRA), asigurând securitatea produselor de la proiectare până la etapele post-comercializare.
8. CRACY: CRACY (CRA made Easy) ajută IMM-urile europene să îndeplinească cerințele Regulamentului UE privind reziliența cibernetică (CRA) prin simplificarea conformității pentru produsele cu elemente digitale, promovarea celor mai bune practici și a produselor și serviciilor mai sigure.

Anexa G: Relația cu alte acte legislative ale UE

Deși nu este posibil să se prezinte în acest document o discuție completă privind relația dintre CRA și alte acte legislative ale UE, unele dintre cele mai importante legături sunt menționate mai jos:

1. *Noul cadru legislativ (CE/2008/765 și CE:2008/768):* CRA se bazează pe NLF și, în esență, extinde cadrul pentru a acoperi produsele cu elemente digitale. Acest lucru este descris în detaliu în secțiunea 4.1 din prezentele orientări.
2. *Reziliența cibernetică:* Atât Directiva NIS2, cât și Regulamentul DORA vizează îmbunătățirea rezilienței cibernetice în întreaga UE. Acestea stabilesc gestionarea riscurilor de securitate cibernetică și raportarea incidentelor de către entitățile care furnizează servicii esențiale. CRA completează aceste inițiative prin impunerea de cerințe de securitate referitoare la produsele cu elemente digitale, contribuind la cadrul de reglementare al UE privind produsele.
3. *Directiva privind echipamentele radio (RED) (Directiva 2014/53/UE)* se concentrează pe siguranța, compatibilitatea electromagnetică și interoperabilitatea produselor echipate cu echipamente radio. CRA se concentrează pe securitatea cibernetică și are un domeniu de aplicare mai larg (inclusiv software-ul, nu numai IoT). Aceasta înlocuiește actul delegat RED pentru securitatea cibernetică.
4. *Regulamentul privind echipamentele tehnice (Regulamentul (UE) 2023/1230)* se referă la sănătatea și siguranța utilizării echipamentelor tehnice. Acesta completează CRA, care se aplică componentelor digitale ale echipamentelor tehnice. Ambele regulamente se aplică simultan.
5. *GDPR al UE:* CRA se bazează pe GDPR, care impune protecția și minimizarea oricăror date (personale sau nu) prelucrate de produsele cu elemente digitale introduse pe piața UE.
6. *Regulamentul privind Inteligența Artificială* (Regulamentul (UE) 2024/1689) reglementează fiabilitatea și siguranța sistemelor (AI). Se aplică funcționalităților IA cu risc ridicat, în timp ce CRA se aplică securității cibernetice a produsului în sine. Un sistem IA cu risc ridicat trebuie să respecte atât Regulamentul privind Inteligența Artificială, cât și cerințele CRA în materie de securitate cibernetică.
7. *Regulamentul UE privind serviciile digitale (DSA) și Regulamentul UE privind piețele digitale (DMA)* impun responsabilitatea platformelor și moderarea conținutului (DSA) și echitatea pieței pentru operatorii de piață (DMA). CRA nu se suprapune direct cu aceste reglementări, dar se aplică software-ului utilizat de platforme și sistemele backend.
8. *Regulamentul privind securitatea cibernetică (CSA)* (Regulamentul (UE) 2019/881): CRA se referă la sistemele de certificare elaborate în temeiul CSA în conformitate cu cerințele de evaluare a conformității (a se vedea secțiunea 4 din

prezentele orientări pentru detalii).