SECURE
Cyber Resilience for SMEs

Cadrul metodologic de evaluare a conformității CRA

20/10/2025

Funded by the European Union

Declarație privind finanțarea: Finanțat de Uniunea Europeană în temeiul Acordului de grant nr. 101190325. Opiniile Și punctele de vedere exprimate aparțin exclusiv autorului/autorilor și nu reflectă neapărat poziția Uniunii Europene sau a Centrului European de Competențe Industriale, Tehnologice și de Cercetare în domeniul Securității Cibernetice. Nici Uniunea Europeană, nici autoritatea care acordă finanțarea nu pot fi considerate responsabile Pentru acestea.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Declarație ECCC: Proiectul este sprijinit de Centrul European de Competențe în Domeniul securității cibernetice și de membri acestuia.

DECLINAREA RESPONSABILITĂȚII

Acest document face parte din livrabilul D4.1, „Ghiduri și materiale pentru conformitatea IMM-urilor cu CRA", al proiectului SECURE.

Prim autor: Autoritatea pentru Digitalizarea României – NCC-RO (ADR-NCC-RO)

Al doilea autor: Centre for Cybersecurity Belgium (CCB)

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cuprins

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Lista tabelelor și figurilor

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Listă de abrevieri

AES - Standard de criptare avansată

API - Interfață de programare a aplicațiilor

CI / CD - Integrare continuă și livrare/dezvoltare continuă

CIS - Centrul pentru Securitatea Internetului

CRA - Actul privind reziliența cibernetică

CSIRT - Echipă de răspuns la incidente de securitate informatică

CVD - Divulgarea coordonată a vulnerabilităților

CVE - Vulnerabilități și expuneri comune

CVSS - Sistem comun de evaluare a vulnerabilităților

CWS - Enumerarea comună a slăbiciunilor

DDoS - Atac distribuit de tip refuz al serviciului

DMS - Sistem de management al documentelor

DPIA - Evaluarea impactului asupra protecției datelor

ECDSA - Algoritm de semnătură digitală cu curbă eliptică

ENISA - Agenția Uniunii Europene pentru Securitate Cibernetică

ETSI - Institutul European de Standarde Tehnice

EU - Uniunea Europeană

EU DoC - Declarația de conformitate UE

EUCS - Securitatea cloud a UE

FTP - Protocol de transfer de fișiere

GDPR - Regulamentul general privind protecția datelor

IDS - Sistem de detectare a intruziunilor

IEC - Comisia Electrotehnică Internațională

IoT - Internetul lucrurilor

IPS - Sistem de prevenire a intruziunilor

ISO - Organizația Internațională de Standardizare

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

MFA - Autentificare multifactor

NB - Organism notificat

NIST - Institutul Național de Standarde și Tehnologie (Statele Unite)

NIST NVD - Baza națională de date privind vulnerabilitățile a NIST

OCTAVE - Evaluarea amenințărilor, activelor și vulnerabilităților critice operațional

OTA - Prin rețea, de la distanță

OWASP - Proiectul deschis la nivel mondial pentru securitatea aplicațiilor

OWASP ESAPI - API pentru securitatea aplicațiilor enterprise OWASP

OWASP SAMM - Modelul de maturitate pentru asigurarea software OWASP

OWASP ZAP - Proxy Zed Attack OWASP

PASTA - Proces pentru simularea atacurilor și analiza amenințărilor

PDE - Produs cu elemente digitale

PSIRT - Echipă de răspuns la incidente de securitate a produsului

RBAC - Control al accesului bazat pe roluri

SBOM - Lista componentelor software

SDLC - Ciclul de viață al dezvoltării securizate

SIEM - Managementul informațiilor și evenimentelor de securitate

IMM - Întreprindere mică și mijlocie

SNMP - Protocol simplu de management al rețelei

SPDX - Schimb de date privind pachetele de sistem

SQL - Limbaj structurat de interogare

SSL - Strat de soclu securizat

STRIDE - Falsificare, modificare neautorizată, repudiere, divulgare de informații, refuz al serviciului, escaladare a privilegiilor

TLS - Securitatea stratului de transport

UpnP - Conectare și redare universală

VPN - Rețea privată virtuală

XSS - Scriptare între site-uri

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Introducere

Actul privind reziliența cibernetică al Uniunii Europene (CRA), Regulamentul (UE) 2024/2847, instituie un cadru cuprinzător pentru a se asigura că produsele cu elemente digitale (PDE) sunt securizate pe întregul lor ciclu de viață, de la proiectare până la sfârșitul perioadei de utilizare. Pentru a sprijini întreprinderile mici și mijlocii (IMM-uri) în evaluarea și îmbunătățirea stadiului lor de conformitate cu CRA, acest document oferă un cadru metodologic de autoevaluare a conformității. El face parte din materialele furnizate de proiectul SECURE[1], care urmărește să sprijine IMM-urile în implementarea CRA.

Prin intermediul unui cadru detaliat, sunt dezvoltate cinci criterii-cheie: (1) conformitatea cu cerințele esențiale de securitate cibernetică, (2) certificarea produselor cu elemente digitale, (3) clasificarea produselor ca produs de Clasa I sau Clasa II și acțiunile corespunzătoare, (4) caracterul complet al documentației tehnice și (5) procedurile generale de evaluare a conformității. Fiecare secțiune este completată cu orientări aprofundate, exemple practice, studii de caz, liste de verificare, referințe la modele, instrumente și standarde, astfel încât IMM-urile să poată parcurge în mod eficient obligațiile CRA prin strategii acționabile, adaptate constrângerilor lor de resurse.

Totuși, toate acestea rămân de natură orientativă și oferă recomandări bazate pe abordări recunoscute și pe bune practici, pentru a sprijini IMM-urile în traiectoria lor de conformare. Referințele la instrumente și cadre existente trebuie tratate ca ilustrative. Acest ghid poate fi actualizat pe măsură ce cadrul legislativ al CRA se dezvoltă în continuare.

[1] Proiectul „Strengthening EU SMEs Cyber Resilience" (SECURE) oferă sprijin financiar și orientare IMM-urilor pentru conformarea cu CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cadrul metodologic de evaluare a conformității CRA

1 Conformitatea cu cerințele esențiale de securitate cibernetică

Criteriul privind conformitatea cu cerințele esențiale de securitate cibernetică reprezintă piatra de temelie a conformității CRA, asigurând că produsele cu elemente digitale îndeplinesc standarde stricte de securitate cibernetică pentru a putea fi introduse pe piața UE. Anexa I la CRA specifică 13 cerințe de securitate cibernetică ale produsului și 8 cerințe privind gestionarea vulnerabilităților, în total 21 de cerințe esențiale. Această secțiune oferă o metodologie exhaustivă pentru IMM-uri, pentru evaluarea conformității, documentarea dovezilor, identificarea lacunelor și dezvoltarea planurilor de remediere. Include explicații detaliate, instrumente practice, studii de caz, modele și orientări pas cu pas pentru a asigura o evaluare și o conformare riguroasă.

1.1 Cerințele de securitate cibernetică ale produsului

Cerințele de securitate cibernetică ale produsului impun ca produsele să fie proiectate și dezvoltate având securitatea ca principiu central („securizat prin proiectare și în mod implicit"). Aceste cerințe asigură că produsele nu conțin vulnerabilități exploatabile cunoscute, au configurații implicite securizate, susțin actualizări de securitate prompte și protejează confidențialitatea, integritatea și disponibilitatea datelor. Mai jos este prezentată o analiză cuprinzătoare a cerințelor[2], cu orientări detaliate, exemple, instrumente și metodologii.

1.1.1 Fără vulnerabilități exploatabile cunoscute

Producătorii trebuie să se asigure că produsele nu conțin vulnerabilități exploatabile cunoscute la momentul lansării, ceea ce presupune testare riguroasă înainte de lansare, inclusiv scanări de vulnerabilități, teste de penetrare și revizuiri de cod. IMM-urile, care se confruntă adesea cu constrângeri de resurse, pot utiliza instrumente eficiente din punct de vedere al costurilor pentru testare și scanare de securitate, cum ar fi scanere dinamice pentru aplicații web, scanere de vulnerabilități de rețea, instrumente de testare statică a securității aplicațiilor și scanere pentru imagini de containere, pentru a identifica problemele. De exemplu, un producător de încuietori inteligente ar trebui să testeze

[2] Unele cerințe suprapuse din Anexa I la CRA sunt grupate împreună în acest ghid, rezultând o listă de opt obligații concrete

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

vulnerabilități Bluetooth, cum ar fi protocoale de împerechere slabe sau atacuri de tip replay, și să documenteze remedierea într-un registru de management al vulnerabilităților. Testarea ar trebui să fie aliniată cu standarde precum OWASP Top 10 sau CWE/SANS Top 25 pentru a acoperi vulnerabilitățile comune.

Orientări detaliate:

- **Scanarea vulnerabilităților:** utilizați OpenVAS sau Nessus pentru scanarea CVE-urilor, programând scanări bilunare în timpul dezvoltării. IMM-urile pot accesa niveluri gratuite ale unor instrumente precum Trivy pentru aplicații bazate pe containere.
- **Testarea de penetrare:** efectuați teste manuale sau automate cu instrumente precum Metasploit sau implicați furnizori terți pentru evaluări trimestriale. Concentrați-vă asupra zonelor cu risc ridicat, cum ar fi autentificarea sau interfețele de rețea.
- **Revizuiri de cod:** utilizați SonarQube pentru detectarea vulnerabilităților la nivel de cod, precum injecția SQL sau cross-site scripting (XSS). Implementați revizuiri inter pares pentru componentele critice.
- **Documentare:** mențineți un registru de management al vulnerabilităților cu coloane pentru ID-ul CVE, scorul CVSS, componenta afectată, acțiunea de remediere și status. Folosiți instrumente precum Jira sau Trello pentru urmărire.
- **Plan de remediere:** pentru vulnerabilitățile nepregătite, prioritizați pe baza scorurilor CVSS, de exemplu peste 7,0 ca fiind critic, și stabiliți termene de remediere, de exemplu 30 de zile pentru problemele critice.

Studiu de caz: Un IMM care dezvoltă un termostat inteligent efectuează o scanare de vulnerabilități cu Nessus și identifică un protocol de criptare slab, TLS 1.1. IMM-ul face upgrade la TLS 1.3, testează remedierea cu OWASP ZAP și documentează procesul într-un registru, incluzând scorurile CVSS și rapoartele de testare. Autoevaluarea confirmă că nu mai există vulnerabilități cunoscute, fiind susținută de un raport de testare de penetrare de la un furnizor terț.

Tabel 1 - Model de registru pentru managementul vulnerabilităților

ID CVE	Scor CVSS	Componentă	Descriere	Acțiune de remediere	Status	Dată Rezolvării
CVE-2025-1234	8.5	TLS 1.1	Criptare slabă	Actualizat la TLS 1.3	Rezolvat	2025-06-15

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.1.2 Configurații implicite securizate

Produsele trebuie livrate cu setări implicite consolidate pentru a minimiza riscurile, cum ar fi dezactivarea serviciilor inutile, utilizarea parolelor puternice și închiderea porturilor deschise. IMM-urile ar trebui să se alinieze cu ETSI EN 303 645, care oferă orientări specifice pentru IoT, sau cu CIS Benchmarks pentru tehnologii specifice, precum Linux sau Docker. De exemplu, o cameră inteligentă pentru locuință ar trebui să dezactiveze accesul la distanță în mod implicit, să solicite parole unice și să închidă porturi neutilizate precum Telnet.

Orientări detaliate:

- **Revizuirea configurației:** elaborați o listă de verificare bazată pe ETSI EN 303 645, verificând setări precum moduri de depanare dezactivate, lipsa credențialelor implicite și porturi închise. Utilizați instrumente care efectuează verificări de consolidare a sistemului.
- **Scanarea porturilor:** utilizați Nmap pentru a identifica porturile și serviciile deschise, asigurându-vă că sunt active doar cele necesare. De exemplu, dezactivați FTP dacă nu este necesar.
- **Politici de parole:** implementați parole implicite puternice sau obligați utilizatorii să le seteze în timpul configurării. Utilizați verificatoare de complexitate a parolelor.
- **Documentare:** includeți setările de configurație în dosarul tehnic, cu referire la standarde precum CIS Benchmarks. Documentați abaterile și justificările.
- **Ghid pentru utilizatori:** furnizați instrucțiuni de configurare în manualele utilizatorului, explicând cum se mențin configurațiile securizate, de exemplu dezactivarea rețelei Wi-Fi pentru oaspeți.

Studiu de caz: Un IMM care produce un router Wi-Fi se asigură că setările implicite dezactivează UPnP și Telnet, utilizând Nmap pentru a verifica porturile închise. Lista de verificare a autoevaluării confirmă conformitatea cu clauza 5.1 din ETSI EN 303 645, susținută de un raport de configurație și de instrucțiuni în manualul utilizatorului.

Tabel 2 - Model de listă de verificare a configurațiilor

Setare	Cerință	Status	Dovezi	Note
UPnP	Dezactivat	Conform	Raport scanare Nmap	Verificat 2025-06-10

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.1.3 Actualizări de securitate prompte

Produsele trebuie să suporte actualizări automate de securitate, cu opțiuni de renunțare pentru utilizatori. IMM-urile pot utiliza mecanisme de actualizare over-the-air (OTA) prin platforme precum Mender.io, AWS IoT Device Management sau Balena. Actualizările trebuie semnate și verificate cu instrumente precum OpenSSL pentru a preveni manipularea. De exemplu, un producător de dispozitive purtabile ar trebui să asigure că actualizările de firmware remediază vulnerabilitățile în termen de 30 de zile de la descoperire, cu notificări clare pentru utilizatori.

Orientări detaliate:

- **Infrastructură de actualizare:** configurați un server OTA sau utilizați soluții cloud. Asigurați semnarea actualizărilor cu RSA-2048 sau ECDSA.
- **Testarea actualizărilor:** verificați că actualizările se instalează fără a perturba funcționalitatea, utilizând medii de testare precum Docker. Efectuați teste de regresie pentru compatibilitate.
- **Notificarea utilizatorilor:** utilizați e-mail, notificări în aplicație sau indicatoare LED pentru a informa utilizatorii despre actualizări. Furnizați instrucțiuni de renunțare în manualele utilizatorului.
- **Documentare:** includeți frecvența actualizărilor, mecanismele de semnare și procedurile de notificare a utilizatorilor în dosarul tehnic. Înregistrați istoricul actualizărilor cu marcaje temporale și CVE-uri abordate.
- **Metrici de conformitate:** urmăriți timpul de implementare a actualizărilor, de exemplu sub 30 de zile pentru patch-uri critice, și rata de adoptare de către utilizatori.

Studiu de caz: Un IMM producător de boxe inteligente utilizează Mender.io pentru a transmite actualizări de firmware semnate, remediind un CVE în 25 de zile. Autoevaluarea documentează procesul OTA, notificarea utilizatorilor prin e-mail și rezultatele testelor de regresie, asigurând conformitatea cu cerințele CRA.

Tabel 3 - Model de registru al actualizărilor

Actualizare ID	CVE Abordat	Data lansării	Timp de implementare	Notificare Utilizator	Status
V2.1.3	CVE 2025-5678	2025-07-01	25 days	Email trimis 2025-06-30	Implementat

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.1.4 Protecție împotriva accesului neautorizat

Mecanismele puternice de autentificare, cum ar fi autentificarea multi-factor (MFA), OAuth 2.0 sau OpenID Connect, sunt esențiale pentru prevenirea accesului neautorizat. IMM-urile pot utiliza JSON Web Tokens (JWT) pentru securitatea API-urilor și controlul accesului bazat pe roluri (RBAC) pentru limitarea permisiunilor. Instrumente precum Burp Suite sau Postman pot simula atacuri pentru testarea controalelor de acces. De exemplu, un dispozitiv IoT conectat la cloud ar trebui să solicite MFA pentru conturile utilizatorilor și să folosească JWT pentru endpoint-urile API.

Orientări detaliate:

- **Implementarea autentificării:** utilizați biblioteci MFA precum Auth0 sau Okta pentru conturile utilizatorilor. Implementați JWT pentru API-uri, conform RFC 7519.
- **Testarea controalelor de acces:** efectuați teste de penetrare cu Burp Suite pentru a simula atacuri de tip brute-force sau deturnare de sesiune. Utilizați instrumente precum Wireshark pentru monitorizarea traficului de rețea.
- **Documentarea politicilor:** includeți politicile de autentificare și control al accesului în dosarul tehnic, detaliind protocoalele și configurațiile RBAC.
- **Monitorizarea accesului:** activați jurnalizarea încercărilor de acces folosind Syslog sau ELK Stack, cu alerte pentru activități suspecte, cum ar fi multiple autentificări eșuate.
- **Audituri regulate:** programați audituri trimestriale ale controalelor de acces, utilizând instrumente precum HashiCorp Vault pentru managementul credențialelor.

Studiu de caz: Un IMM care dezvoltă o sonerie inteligentă implementează MFA folosind Auth0 și o testează cu Burp Suite, identificând și remediind o deficiență de management al sesiunilor. Autoevaluarea include politicile de autentificare, rapoartele de testare și configurațiile de jurnalizare.

Tabel 4 - Model de politică de control al accesului

Componentă	Autentificare	Control acces	Metodă testare	Dovezi	Status
Logare utilizator	MFA (Auth0)	RBAC (Admin/utilizator)	Burp Suite	Raport test 2025-06-20	Conform

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.1.5 Confidențialitatea, integritatea și disponibilitatea datelor

Criptarea este esențială pentru protejarea datelor. IMM-urile ar trebui să implementeze AES-256 pentru datele în repaus și TLS 1.3 pentru datele în tranzit, în aliniere cu NIST SP 800-52. Validarea intrărilor ar trebui să prevină atacurile de injecție, folosind biblioteci precum OWASP ESAPI. De exemplu, un dispozitiv de monitorizare a sănătății trebuie să cripteze datele pacienților pentru a se conforma cu GDPR și CRA, asigurând confidențialitatea și integritatea.

Orientări detaliate:

- **Selectarea standardelor de criptare:** utilizați AES-256 pentru stocare și TLS 1.3 pentru comunicații. Implementați managementul cheilor cu AWS KMS sau HashiCorp Vault.
- **Testarea criptării:** efectuați teste de penetrare cu Metasploit pentru a verifica protecția datelor. Utilizați instrumente precum SSL Labs pentru evaluarea configurațiilor TLS.
- **Validarea intrărilor:** implementați validarea intrărilor cu ESAPI sau biblioteci similare pentru a preveni injecțiile SQL sau XSS.
- **Documentarea criptării:** includeți protocoalele de criptare, politicile de management al cheilor și rezultatele testelor în dosarul tehnic.
- **Monitorizarea disponibilității:** utilizați instrumente de monitorizare precum Nagios pentru a asigura disponibilitatea sistemului și reziliența împotriva atacurilor DDoS.

Studiu de caz: Un IMM producător de dispozitive medicale criptează datele pacienților cu AES-256 și TLS 1.3, testează cu Metasploit și documentează conformitatea în dosarul tehnic. Validarea intrărilor previne injecțiile SQL, verificată prin scanări OWASP ZAP.

Tabel 5 - Model de conformitate privind criptarea

Tip de date	Criptare	Gestionarea cheilor	Metoda de testare	Dovezi	Status
Date pacient	AES-256	AWS KMS	Metasploit	Raport test 2025-06-25	Conform

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.1.6 Minimizarea datelor și reducerea suprafeței de atac

Produsele ar trebui să colecteze doar datele necesare și să minimizeze interfețele deschise. IMM-urile pot utiliza Nmap pentru scanarea porturilor deschise și OWASP Dependency-Check pentru identificarea dependențelor neutilizate. O evaluare a impactului asupra protecției datelor (DPIA), aliniată cu GDPR, ar trebui să justifice colectarea datelor. De exemplu, un tracker de fitness ar trebui să limiteze datele la ritmul cardiac și pași, dezactivând serviciile Bluetooth neutilizate.

Orientări detaliate:

- **Maparea fluxurilor de date:** efectuați o DPIA pentru documentarea colectării, prelucrării și stocării datelor. Utilizați instrumente precum OneTrust pentru automatizarea DPIA.
- **Minimizarea interfețelor:** utilizați Nmap pentru identificarea și închiderea porturilor sau API-urilor inutile. Dezactivați protocoale neutilizate precum SNMP sau FTP.
- **Eliminarea dependențelor:** utilizați Dependency-Check pentru identificarea și eliminarea bibliotecilor neutilizate.
- **Documentarea minimizării:** includeți rezultatele DPIA și configurațiile interfețelor în dosarul tehnic.
- **Revizuiri regulate:** programați actualizări trimestriale ale DPIA pentru a reflecta modificările produsului.

Studiu de caz: Un IMM producător de trackere de fitness efectuează o DPIA, limitează colectarea datelor la metrici esențiale și dezactivează serviciile Bluetooth neutilizate. Scanările Nmap confirmă o suprafață de atac minimă, documentată în autoevaluare.

Tabel 6 - Model de rezumat DPIA

Tip de Date	Scop	Necesitate	Acțiune de minimizare	Dovezi	Status
Ritm cardiac	Monitorizare a sănătății	Esențial	Dezactivarea urmăririi locației	Raport DPIA 2025-06-30	Conform

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.1.7 Atenuarea incidentelor și jurnalizarea

Produsele trebuie să includă mecanisme pentru limitarea daunelor cauzate de incidente, precum limitarea ratei sau detecția intruziunilor, și să permită jurnalizarea securizată. IMM-urile pot utiliza instrumente de jurnalizare, asigurând stocare rezistentă la manipulare. De exemplu, un router de rețea ar trebui să jurnalizeze încercările de acces neautorizat și să implementeze limitarea ratei pentru prevenirea atacurilor brute-force.

Orientări detaliate:

- **Implementarea atenuării:** utilizați limitarea ratei, de exemplu prin NGINX, și sisteme de detecție a intruziunilor precum Snort.
- **Activarea jurnalizării:** configurați Syslog sau ELK Stack pentru jurnalizare securizată, criptată. Stabiliți politici de retenție, de exemplu 6 luni.
- **Testarea atenuării:** simulați atacuri cu instrumente precum hping3 pentru verificarea eficienței limitării ratei și IDS.
- **Documentarea jurnalelor:** includeți formatele de jurnal, politicile de retenție și rezultatele testelor în dosarul tehnic.
- **Revizuirea jurnalelor:** programați revizuiri lunare ale jurnalelor pentru identificarea anomaliilor, folosind instrumente precum Splunk pentru analiză.

Studiu de caz: Un IMM producător de routere implementează limitarea ratei cu NGINX și jurnalizează încercările de acces cu ELK Stack. Testele de penetrare cu hping3 confirmă atenuarea, documentată în autoevaluare.

Tabel 7 - Model de configurare a jurnalizării

Tip eveniment	Format jurnal	Stocare	Retenție	Metoda de testare	Dovezi	Status
Access Attempts	Syslog	criptată	6 luni	hping3	Raport test 2025-07-01	Conform

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.1.8 Ștergerea datelor utilizatorilor

Produsele trebuie să permită utilizatorilor să șteargă în mod securizat datele personale, folosind tehnici de ștergere criptografică. De exemplu, o boxă inteligentă ar trebui să ofere o opțiune de resetare la setările din fabrică care suprascrie datele utilizatorului cu instrumente precum o bibliotecă criptografică pentru ștergere securizată. IMM-urile ar trebui să verifice eficacitatea ștergerii cu instrumente criminalistice.

Orientări detaliate:

- **Implementarea ștergerii:** furnizați o opțiune de resetare securizată, folosind ștergere criptografică, de exemplu OpenSSL s_random.
- **Testarea ștergerii:** utilizați instrumente criminalistice pentru a verifica dacă datele nu mai pot fi recuperate.
- **Documentarea procesului:** includeți instrucțiunile de ștergere și rezultatele testelor în dosarul tehnic.
- **Ghid pentru utilizatori:** furnizați instrucțiuni clare în manuale, cu suport online pentru depanare.
- **Testare regulată:** programați teste anuale pentru a vă asigura că mecanismele de ștergere rămân eficiente.

Studiu de caz: Un IMM producător de boxe inteligente implementează o resetare la setările din fabrică cu ștergere criptografică, testată cu Autopsy. Autoevaluarea include instrucțiuni din manualul utilizatorului și rapoarte de testare.

Tabel 8 - Model de verificare a ștergerii datelor

Componentă	Metodă de ștergere	Instrument de testare	Dovezi	Status
Date utilizator	Ștergere criptografică	Autopsie	Raport test 2025-07-05	Conform

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.2 Cerințe privind gestionarea vulnerabilităților

Cele 8 cerințe privind gestionarea vulnerabilităților asigură managementul continuu al securității după lansare, impunând procese pentru identificarea, remedierea și divulgarea vulnerabilităților. Mai jos este prezentată o analiză detaliată a cerințelor[3].

1.2.1 Lista materialelor software (SBOM)

Producătorii trebuie să mențină un SBOM citibil automat, în formate precum CycloneDX sau SPDX. Instrumente precum Snyk, Dependabot sau Trivy pot automatiza generarea SBOM. De exemplu, un IMM care dezvoltă o aplicație web utilizează Dependabot pentru a urmări dependențele și pentru a genera un SBOM, asigurând transparența componentelor terțe.

Orientări detaliate:

- **Generarea SBOM:** utilizați Snyk sau Trivy pentru a crea un SBOM, incluzând numerele de versiune și licențele.
- **Actualizarea SBOM:** programați actualizări lunare pentru a reflecta componentele sau patch-urile noi.
- **Verificarea componentelor:** verificați vulnerabilitățile utilizând NVD al NIST sau baza de date Snyk.
- **Documentarea SBOM:** includeți SBOM-ul în dosarul tehnic, cu un jurnal al modificărilor pentru actualizări.
- **Integrarea în CI/CD:** utilizați instrumente precum GitHub Actions pentru automatizarea generării SBOM în pipeline-urile de dezvoltare.

Studiu de caz: Un IMM furnizor de servicii cloud generează un SBOM cu CycloneDX, identificând o bibliotecă vulnerabilă, Log4j. IMM-ul aplică patch-ul, actualizează SBOM-ul și documentează procesul în autoevaluare.

Tabel 9 - Model de rezumat SBOM

Componentă	Versiune	Licență	Vulnerabilitate	Acțiune	Status
Log4j	2.16.0	Apache 2.0	CVE-2021-44228	Actualizat la 2.17.1	Rezolvat

[3] După cum s-a menționat mai sus, pentru a evita suprapunerile, unele cerințe au fost regrupate, rezultând o listă de șase obligații.

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.2.2 Remedierea la timp a vulnerabilităților

Vulnerabilitățile trebuie abordate fără întârzieri nejustificate, prioritizând problemele critice pe baza scorurilor CVSS. IMM-urile ar trebui să lanseze patch-uri în termen de 30 de zile pentru vulnerabilitățile critice și în termen de 60 de zile pentru celelalte. De exemplu, un IMM producător de camere inteligente aplică patch-ul pentru un CVE în 25 de zile și notifică utilizatorii prin e-mail.

Orientări detaliate:

- **Monitorizarea vulnerabilităților:** utilizați Snyk, NVD al NIST sau VulnDB pentru urmărirea CVE-urilor.
- **Prioritizarea patch-urilor:** utilizați scorurile CVSS pentru prioritizare, de exemplu peste 7,0 ca critic și 4,0-6,9 ca mediu.
- **Testarea patch-urilor:** efectuați teste de regresie într-un mediu sandbox pentru a asigura stabilitatea.
- **Notificarea utilizatorilor:** folosiți e-mail, notificări în aplicație sau avize pe website pentru informarea utilizatorilor.
- **Documentarea remedierii:** includeți termenele patch-urilor, rezultatele testelor și notificările către utilizatori în dosarul tehnic.

Studiu de caz: Un IMM producător de încuietori inteligente identifică un CVE critic, cu scor CVSS 8,8, și lansează un patch în termen de 20 de zile, documentând procesul și notificarea utilizatorilor.

Tabel 10 - Model de registru pentru remedierea vulnerabilităților

ID CVE	Scor CVSS	Componentă	Data Patch-ului	Metoda de Notificare	Status
CVE-2025-5678	8.8	Firmware	2025-07-01	Email	Rezolvat

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.2.3 Testare de securitate regulată

Este necesară testare periodică, inclusiv teste de penetrare, scanări de vulnerabilități și revizuiri de cod. IMM-urile pot utiliza OpenVAS, Nessus sau furnizori terți pentru audituri eficiente din punct de vedere al costurilor, programând scanări trimestriale și teste de penetrare anuale.

Orientări detaliate:

- **Programarea testelor:** planificați scanări trimestriale de vulnerabilități și teste de penetrare anuale, în aliniere cu ISO 27001 Anexa A.12.6.1.
- **Utilizarea instrumentelor:** folosiți OpenVAS pentru scanări, Burp Suite pentru aplicații web sau Metasploit pentru testare de penetrare.
- **Documentarea rezultatelor:** includeți rapoartele de testare, constatările și planurile de remediere în dosarul tehnic.
- **Remedierea constatărilor:** prioritizați problemele în funcție de severitate și stabiliți termene de remediere.
- **Automatizarea testării:** integrați instrumente precum Snyk în pipeline-uri CI/CD pentru scanare continuă.

Studiu de caz: Un IMM producător de dispozitive smart home efectuează scanări trimestriale OpenVAS și un test anual de penetrare cu un furnizor terț, documentând rezultatele și planurile de remediere în autoevaluare.

Tabel 11 - Model de calendar de testare a securității

Tip de test	Frecvență	Instrument	Ultima efectuare	Constatări	Status Remediere
Scanare vulnerabilități	Trimestrial	OpenVAS	2025-06-30	2 CVEs	Rezolvat

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.2.4 Transparență în divulgarea vulnerabilităților

Producătorii trebuie să divulge public detaliile vulnerabilităților și actualizările de remediere după ce patch-urile sunt disponibile. IMM-urile ar trebui să publice avize de securitate pe website-ul propriu, detaliind severitatea, impactul, versiunile afectate, măsurile de atenuare sau soluțiile temporare și calendarul, în conformitate cu standarde și bune practici recunoscute pentru divulgarea vulnerabilităților, de exemplu ISO/IEC 29147 și ISO/IEC 30111, ghidurile ENISA CVD, orientările FIRST pentru coordonarea multipartită sau o politică internă echivalentă care se mapează la acestea.

Orientări detaliate:

- **Crearea unui model de divulgare:** dezvoltați un format standard pentru avize, incluzând ID-ul CVE, scorul CVSS, impactul și detaliile patch-ului.
- **Publicarea avizelor:** postați pe website-ul companiei, blog sau portal de securitate.
- **Notificarea utilizatorilor:** utilizați e-mail, notificări în aplicație sau social media pentru informarea utilizatorilor.
- **Documentarea divulgărilor:** includeți un link sau o cale DMS către arhiva publică de avize, jurnalul intern de modificări pentru textul avizului și dovada notificărilor către utilizatori, liste, marcaje temporale și canale.
- **Implicarea coordonatorilor:** acolo unde este adecvat, partajați avizele cu CSIRT-uri/PSIRT-uri naționale relevante sau comunități și arhive de coordonare a vulnerabilităților pentru a sprijini conștientizarea largă, folosind canale neutre, fără a impune un anumit brand.
- **Precizarea bazei:** în politica publică, menționați ghidul cu care vă aliniați, de exemplu ISO/IEC 29147 și ISO/IEC 30111 sau bunele practici ENISA CVD, și notați că sunt acceptate procese echivalente funcțional. Păstrați versiunea/data politicii și revizuiți-o anual.

Studiu de caz: Un IMM producător de televizoare inteligente publică un aviz de securitate pentru un CVE, detaliind patch-ul și impactul. Autoevaluarea include avizul și înregistrările de notificare a utilizatorilor.

Tabel 12 - Model de aviz de Securitate

ID CVE	Scor CVSS	Impact	Detalii Patch	Data Publicării	Metodă de Notificare
CVE-2025-1234	7.5	Breșă de date	Firmware v2.1.3	2025-07-01	Website, Email

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Pot fi adăugate și alte coloane, cum ar fi versiuni/build-uri afectate; măsuri de atenuare/soluții temporare, dacă patch-ul nu este încă disponibil; calendarul divulgării, raport primit - confirmat - remediat - publicat; mulțumiri, cercetător/CSIRT, dacă este cazul.

1.2.5 Politica de divulgare coordonată a vulnerabilităților (CVD)

IMM-urile trebuie să ofere un canal clar pentru raportarea vulnerabilităților, cum ar fi o adresă de e-mail dedicată sau un portal web. Platforme precum HackerOne sau Bugcrowd pot facilita CVD prin programe de bug bounty, încurajând hackerii etici să raporteze probleme.

Orientări detaliate:

- **Stabilirea politicii CVD:** creați o politică cu o adresă de e-mail dedicată, de exemplu security@company.com, sau un portal, urmând orientările ISO 29147.
- **Promovarea raportării:** publicați politica pe website-ul companiei și pe forumuri pentru dezvoltatori.
- **Răspuns prompt:** confirmați primirea rapoartelor în termen de 7 zile și furnizați actualizări în termen de 30 de zile.
- **Documentarea politicii:** includeți politica CVD, metricile de răspuns și vulnerabilitățile raportate în dosarul tehnic.
- **Recompensarea raportorilor:** luați în considerare programe de bug bounty pentru stimularea raportării, folosind platforme precum HackerOne.

Studiu de caz: Un IMM configurează un portal CVD pe HackerOne, primind și rezolvând o vulnerabilitate raportată în 25 de zile. Autoevaluarea documentează politica și metricile de răspuns.

Tabel 13 - Model de politică CVD

Canal	hTimp de răspuns	Vulnerabilități raportate	Dovezi	Status
security@company.com	7 zile	3 CVEs	Raport HackerOne	Rezolvat

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.2.6 Actualizări de securitate gratuite

Actualizările trebuie furnizate gratuit pentru o perioadă de suport definită, de exemplu minimum 5 ani pentru dispozitive IoT sau pentru durata de viață a produsului. IMM-urile ar trebui să se asigure că actualizările sunt ușor de instalat, preferabil automat, folosind mecanisme OTA.

Orientări detaliate:

- **Definirea perioadei de suport (CRA art. 13(8)):** stabiliți o perioadă de suport care reflectă durata estimată de utilizare a produsului; aceasta nu poate fi mai scurtă de 5 ani, cu excepția cazului în care produsul este în mod rezonabil așteptat să fie utilizat mai puțin de 5 ani, situație în care perioada de suport este egală cu această durată mai scurtă. Dacă produsul este așteptat să fie utilizat mai mult de 5 ani, stabiliți o perioadă de suport mai lungă.
- **Automatizarea actualizărilor:** utilizați platforme OTA precum Mender.io sau Balena pentru actualizări fluide.
- **Testarea actualizărilor:** verificați instalarea și funcționalitatea actualizărilor într-un mediu de testare.
- **Documentarea suportului:** includeți politicile de suport, registrele de actualizare și instrucțiunile pentru utilizatori în dosarul tehnic.
- **Monitorizarea conformității:** urmăriți implementarea actualizărilor și ratele de adoptare de către utilizatori, asigurându-vă că nu se percep costuri.

Conform cerințelor CRA, producătorul trebuie să se asigure că fiecare actualizare de securitate rămâne disponibilă utilizatorilor pentru o perioadă de cel puțin 10 ani de la emitere sau pentru durata rămasă a perioadei de suport, oricare dintre acestea este mai lungă. În practică, IMM-urile ar trebui să mențină un depozit de arhivă pentru patch-urile de securitate, de exemplu pe website sau pe serverul de actualizări, accesibil clienților chiar și după încheierea suportului oficial. De asemenea, dacă produsul evoluează prin versiuni software majore, producătorul trebuie să ofere utilizatorilor noile versiuni gratuit și fără a impune costuri suplimentare hardware sau software pentru a beneficia de remedierile de securitate, în conformitate cu art. 13(10) CRA. Toate aceste aspecte vor fi documentate în dosarul tehnic, inclusiv justificarea perioadei de suport, minimum 5 ani, și modul în care utilizatorii sunt informați despre sfârșitul suportului sau disponibilitatea pe termen lung a actualizărilor de securitate.

Studiu de caz: Un IMM producător de termostate inteligente se angajează la 5 ani de actualizări gratuite prin Mender.io, documentând politica și mecanismul OTA în autoevaluare.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Tabel 14 - Model de politică de suport

Produs	Perioadă de Suport	Mecanism de actualizare	Ultima actualizare	Dovezi	Status
Termostat	5 years	OTA (Mender.io)	2025-07-01	Registru actualizări	Conform

1.3 Listă de verificare recomandată pentru autoevaluare

Pentru conformarea cu obligațiile CRA privind documentația tehnică și evaluarea conformității, menținerea unei liste de verificare structurate pentru autoevaluare poate oferi un sprijin solid. Recomandăm o singură listă de verificare care acoperă toate cele 21 de cerințe din Anexa I, pentru urmărirea statusului, dovezilor și aprobărilor pe întregul ciclu de viață al produsului. Coloanele unei asemenea autoevaluări pot fi:

- Referință Anexa I / ID cerință, de exemplu 1.1.9 Secure Boot;
- Produs / versiune, inclusiv build firmware/software;
- Declarație de conformitate, Da / Parțial / Nu;
- Dovezi obiective, link/cale, raport de testare, politică, configurație, SBOM, aviz;
- Data testării/revizuirii;
- Rol responsabil / proprietar;
- Abateri și controale compensatorii, dacă există;
- Risc rezidual și justificare;
- Următoarea acțiune / termen-limită;
- Aprobare / semnătură, nume, dată;
- Referință dosar tehnic, locul în care se află în indexul documentației tehnice.

IMM-urile pot utiliza un tablou de bord de conformitate în instrumente precum Confluence, Notion sau Excel pentru a vizualiza progresul, a crea legături către dovezi și a urmări remedierea.

Această listă de verificare este un artefact intern de control destinat să sprijine conformitatea CRA, documentația tehnică, evaluarea conformității și monitorizarea post-piață. Ea nu înlocuiește, în sine, nicio obligație CRA; mai degrabă, organizează dovezile pe care trebuie deja să le produceți și să le mențineți.

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.4 Studiu de caz

Un IMM care dezvoltă o sonerie inteligentă efectuează o autoevaluare:

- **Cerințe ale produsului:** utilizează OWASP ZAP pentru a verifica absența vulnerabilităților, implementează TLS 1.3 și dezactivează porturile neutilizate. Testele de penetrare confirmă conformitatea.
- **Gestionarea vulnerabilităților:** generează un SBOM cu CycloneDX, efectuează scanări trimestriale OpenVAS și publică o politică CVD pe HackerOne.
- **Rezultat:** atinge conformitatea completă cu 18 cerințe, identifică lacune privind actualizările automate și planifică remedierea în termen de 3 luni, documentată într-un tablou de bord.

1.5 Instrumente și resurse

Exemplele și capabilitățile enumerate în acest document sunt independente de instrument. Ele descriu ce trebuie să facă un instrument, nu ce marcă trebuie utilizată. Echipele pot folosi orice soluție echivalentă care furnizează capabilitatea și dovezile indicate.

- **Scanarea vulnerabilităților:** OpenVAS, Nessus, Trivy.
- **Testare de penetrare:** Metasploit, Burp Suite.
- **Analiză de cod:** SonarQube, OWASP Dependency-Check.
- **Jurnalizare:** Syslog, ELK Stack, Graylog.
- **Generare SBOM:** Snyk, CycloneDX, SPDX.
- **Standarde:** ETSI EN 303 645, NIST SP 800-53, ISO 27001.

Această secțiune oferă IMM-urilor o metodologie robustă și detaliată pentru a obține și documenta conformitatea cu toate cerințele esențiale, sprijinită de instrumente practice, modele și studii de caz.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

2 Certificarea produselor care conțin elemente digitale

Criteriul privind certificarea produselor care conțin elemente digitale utilizează scheme europene de certificare a securității cibernetice pentru a demonstra conformitatea cu CRA, în aliniere cu Actul privind securitatea cibernetică (UE) 2019/881. Schemele UE de certificare a securității cibernetice există în temeiul Actului privind securitatea cibernetică, de exemplu EUCC pentru produse TIC, dar rolul lor pentru prezumția de conformitate CRA va fi specificat prin acte delegate ale Comisiei în temeiul art. 27(9).

Prezumția de conformitate (CRA art. 27(8)-(9)): atunci când Comisia specifică, prin act delegat în temeiul CRA, scheme europene aplicabile de certificare a securității cibernetice, produsele care dețin o declarație UE de conformitate sau un certificat în cadrul unei astfel de scheme sunt prezumate conforme doar cu cerințele din Anexa I acoperite de certificatul respectiv. Această secțiune oferă IMM-urilor o metodologie exhaustivă pentru evaluarea aplicabilității certificării, maparea cerințelor CRA la standarde și integrarea certificărilor în autoevaluare, cu orientări detaliate, studii de caz și modele.

2.1 Scheme și standarde de certificare

CRA încurajează certificări precum Common Criteria (ISO/IEC 15408), EUCS (Securitatea cloud a UE), ETSI EN 303 645 pentru IoT și IEC 62443 pentru sisteme industriale. IMM-urile ar trebui să evalueze dacă categoria produsului lor este acoperită de o schemă existentă, folosind resurse precum listele ENISA de candidați la certificare.

Standarde-cheie:

- **ETSI EN 303 645:** acoperă securitatea IoT, inclusiv configurații securizate, protecția datelor și divulgarea vulnerabilităților.
- **Common Criteria:** oferă niveluri de asigurare, EAL1-EAL7, pentru produse IT, adecvate sistemelor critice precum firewall-urile.
- **ISO 27001:** se concentrează asupra proceselor organizaționale de securitate, relevante pentru gestionarea vulnerabilităților.
- **IEC 62443:** abordează IoT industrial, acoperind dezvoltarea și operarea securizată.
- **NIST SP 800-53:** oferă controale tehnice de securitate, mapabile la cerințele CRA.

2.2 Metodologia de autoevaluare

Autoevaluarea ar trebui să includă o listă de verificare detaliată:

1. **Certificări existente:** produsul deține o certificare de securitate cibernetică? De

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

exemplu, un dispozitiv smart home certificat conform ETSI EN 303 645 acoperă multe cerințe CRA.

2. **Aplicabilitate:** produsul este eligibil pentru o schemă europeană de certificare? Consultați listele ENISA sau organismele notificate.
3. **Aliniere cu standardele:** mapați cerințele CRA la standarde, identificând suprapunerile. De exemplu, ISO 27001 A.12.6.1 acoperă gestionarea vulnerabilităților.
4. **Planificarea certificării:** evaluați fezabilitatea obținerii certificării, luând în calcul costurile, termenele și beneficiile.
5. **Conformitate parțială:** documentați aderarea la standarde chiar și fără certificare completă, pentru a demonstra diligență.

Tabel 15 - Exemplu de mapare

Cerință CRA	Standard	Clauză	Dovezi
Configurații implicite securizate	ETSI EN 303 645	Clauză 5.1	Raport de configurație
Divulgarea vulnerabilităților	ISO 27001	A.12.6.1	Politica CVD

2.3 Pași practici pentru IMM-uri

1. **Identificarea standardelor relevante:** utilizați website-ul ENISA sau consultați organisme notificate pentru a găsi standardele aplicabile. De exemplu, un IMM producător de contoare inteligente ar trebui să revizuiască IEC 62443.
2. **Documentarea conformității:** mențineți înregistrări ale aderării la standarde, precum rapoarte de audit ISO 27001 sau rezultate ale testelor ETSI EN 303 645.
3. **Implicarea organismelor de certificare:** contactați organisme acreditate listate de ENISA pentru procesele de certificare.
4. **Valorificarea conformității parțiale:** documentați conformitatea parțială cu standardele pentru a reduce aria evaluării CRA.
5. **Dezvoltarea unei foi de parcurs pentru certificare:** planificați termene, bugete și resurse pentru certificare. De exemplu, certificarea Common Criteria poate dura 6-12 luni și poate costa 50.000-100.000 EUR.

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

2.4 Studiu de caz

Un IMM care dezvoltă o platformă IoT bazată pe cloud urmărește certificarea EUCS:

- **Evaluare:** mapează cerințele CRA la EUCS, identificând suprapuneri privind protecția datelor, criptarea și gestionarea vulnerabilităților.
- **Acțiune:** implică un organism notificat (NB), transmite rapoarte de testare, de exemplu teste de penetrare și SBOM, și documentează conformitatea cu clauzele EUCS.
- **Rezultat:** obține certificarea în 9 luni, simplificând conformitatea CRA și sporind încrederea pieței. Autoevaluarea include un tabel de mapare și raportul de certificare.

2.5 Model de foaie de parcurs pentru certificare

Tabel 16 - Model de foaie de parcurs pentru certificare

Certificare	Calendar	Estimare Cost	Responsabil	Dovezi	Status
EUCS	9 luni (2025-03-01 - 2025-12-01)	€75,000	Echipa de securitate	Rapoarte de testare	În progres

2.6 Instrumente și resurse

- **ENISA:** liste de candidați pentru certificare și directoare ale organismelor notificate.
- **Standarde:** ETSI EN 303 645, ISO 27001, IEC 62443, Common Criteria.
- **Instrumente:** Confluence pentru documentare, Snyk pentru generarea SBOM, OWASP ZAP pentru testare.

Această secțiune asigură că IMM-urile pot utiliza certificările pentru a simplifica conformitatea CRA, cu orientări detaliate, modele și studii de caz.

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

3 Clasificarea produsului: căi de conformitate

Criteriul privind clasificarea produsului determină calea de conformitate adecvată pe baza clasificării CRA bazate pe risc a produselor în Default, Important - Clasa I (Anexa III), Important - Clasa II (Anexa III) și Critic (Anexa IV). Această secțiune oferă o metodologie exhaustivă pentru IMM-uri, pentru clasificarea produselor, înțelegerea obligațiilor de conformitate și integrarea clasificării în autoevaluare, cu orientări detaliate, metodologii de evaluare a riscurilor și studii de caz.

3.1 Înțelegerea clasificării produselor

CRA clasifică produsele în funcție de riscul lor potențial de securitate cibernetică, astfel cum este definit în Anexa III și Anexa IV:

- **Default:** produsul nu este listat în Anexa III/IV.
- **Important - Clasa I (Anexa III):** de exemplu, sisteme de operare, browsere, VPN, SIEM, routere/modemuri.
- **Important - Clasa II (Anexa III):** de exemplu, hipervizoare, runtime-uri pentru containere, firewall-uri, IDS/IPS.
- **Critic (Anexa IV):** de exemplu, dispozitive hardware cu elemente de securitate, gateway-uri pentru contoare inteligente, smartcarduri/elemente securizate.

Clasificarea se bazează pe cazul de utilizare al produsului, sensibilitatea datelor și impactul potențial asupra infrastructurii critice sau siguranței utilizatorilor.

3.2 Metodologia de autoevaluare

Autoevaluarea ar trebui să includă un arbore decizional detaliat:

1. **Verificarea anexelor CRA:** revizuiți Anexa III și IV pentru categoriile de produse. De exemplu, camerele smart home sunt Clasa I, iar software-ul VPN este Clasa II.
2. **Evaluarea impactului riscului:** efectuați o evaluare a riscurilor folosind ISO 27005, NIST SP 800-30 sau OCTAVE Allegro pentru a evalua impactul unui atac cibernetic.
3. **Documentarea clasificării:** înregistrați clasificarea, rezultatele evaluării riscurilor și justificarea în dosarul tehnic.
4. **Verificarea căii de conformitate:** asigurați-vă că se urmează modulul corect de evaluare, control intern sau examinare UE de tip, în funcție de clasificare.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Tabel 17 - Exemplu de arbore decizional

Întrebare	Răspuns	Acțiune
Produsul se află în Anexa III sau IV?	DA (Clasa II)	Implicarea unui organism notificat pentru examinare de tip UE
O defecțiune ar putea afecta infrastructura critică?	Nu	Clasificați produsul ca implicit sau Clasa I și utilizați controlul intern.

3.3 Căi de conformitate

- **Produse Default:** Modul A, control intern al producției. Producătorul autoevaluează conformitatea cu toate cele 21 de cerințe din Anexa I și păstrează documentația tehnică completă.
- **Important - Clasa I:** Modul A numai dacă sunt aplicate standarde armonizate/specificații comune sau o schemă aplicabilă de certificare UE a securității cibernetice, cu nivel de asigurare cel puțin „substantial"; altfel, este necesară evaluare terță parte, Modulele B + C sau H, pentru cerințele neacoperite.
- **Important - Clasa II:** evaluare terță parte obligatorie, Modulele B + C sau H, sau o schemă aplicabilă de certificare UE a securității cibernetice, nivel de asigurare cel puțin „substantial"; Modul A nu este permis.
- **Critic (Anexa IV):** acolo unde este desemnat prin act delegat, certificarea UE de securitate cibernetică este obligatorie, la nivelul de asigurare specificat. Până la o asemenea desemnare, se aplică art. 32(3), aceleași opțiuni ca pentru Important - Clasa II.

3.4 Pași practici pentru IMM-uri

1. **Listă de verificare pentru clasificare:** dezvoltați o listă de verificare pentru a verifica dacă produsul corespunde criteriilor Clasei I sau II, incluzând întrebări privind sensibilitatea datelor, impactul asupra infrastructurii și listările în anexe.
2. **Evaluarea riscurilor:** utilizați OCTAVE Allegro sau NIST SP 800-30 pentru evaluarea riscurilor, concentrându-vă asupra probabilității și impactului. De exemplu, evaluați riscuri precum breșe de date sau manipularea dispozitivului.
3. **Planificarea conformității:** pentru Clasa II, identificați organisme notificate, de exemplu prin ENISA, și bugetați audituri, 50.000-150.000 EUR. Pentru Default/Clasa I, programați audituri interne.

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

4. **Documentare:** includeți rapoartele de clasificare, evaluările de risc și planurile de conformitate în dosarul tehnic.
5. **Revizuiri regulate:** reevaluați anual clasificarea pentru a ține cont de actualizările produsului sau de noile orientări CRA.

Tabel 18 - Model de evaluare a riscurilor

Amenințare	Probabilitate	Impact	Nivel de risc	Atenuare	Dovezi
Acces neautorizat	Medie	ridicat	Ridicat	MFA	Raport test 2025-07-01

3.5 Studiu de caz

Un IMM care dezvoltă un manager de parole, Clasa I, îl clasifică pe baza Anexei III, efectuează o evaluare a riscurilor conform NIST SP 800-30, identificând riscuri precum furtul de credențiale, și implică un organism notificat pentru examinarea UE de tip. Autoevaluarea documentează clasificarea, evaluarea riscurilor și pregătirea auditului, asigurând conformitatea cu cerințele CRA.

3.6 Instrumente și resurse

- **Evaluarea riscurilor:** OCTAVE Allegro, NIST SP 800-30, ISO 27005.
- **Documentare:** Confluence, SharePoint.
- **Organisme notificate:** directorul ENISA.

Această secțiune propune un flux de lucru practic, independent de instrumente, pe care IMM-urile îl pot utiliza pentru clasificarea produselor și alegerea unei căi adecvate de evaluare a conformității CRA. Este o opțiune de sprijin pentru conformitate; organizațiile pot utiliza un flux de lucru echivalent dacă acesta produce aceleași decizii și dovezi. Pașii și artefactele de mai sus sunt recomandări, nu metode impuse de CRA. Acolo unde acest document menționează un „instrument de evaluare a riscului", acesta trebuie înțeles ca un substituent pentru orice metodă care produce rezultatele de capabilitate enumerate, de exemplu o matrice calitativă a riscului sau o fișă de scorare simplificată.

Acest ghid va fi actualizat pe măsură ce actele de punere în aplicare/delegate și schemele de certificare ale UE vor fi finalizate. Până atunci, tratați fluxurile de lucru de mai sus ca opțiuni ilustrative pentru structurarea clasificării interne și colectarea dovezilor.

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

4 Documentația tehnică și evaluarea riscurilor

Criteriul privind documentația tehnică și evaluarea riscurilor asigură că IMM-urile produc documentație cuprinzătoare pentru a demonstra conformitatea CRA. CRA solicită un dosar tehnic pentru fiecare produs, incluzând descrierea produsului, evaluări ale riscurilor, măsuri de securitate, rapoarte de testare și ghiduri pentru utilizatori. Această secțiune oferă o metodologie exhaustivă pentru compilarea și evaluarea documentației, cu orientări detaliate, modele și studii de caz.

4.1 Cerințe de documentare

Dosarul tehnic trebuie să includă:

6. **Descrierea produsului:** specificații detaliate, funcționalitate și utilizare intenționată.
7. **Evaluarea riscurilor:** analiză cuprinzătoare a amenințărilor și măsurilor de atenuare, aliniată cu ISO 27005 sau NIST SP 800-30.
8. **Conformitatea cu cerințele esențiale:** dovezi ale conformității cu toate cele 21 de cerințe, inclusiv rapoarte de testare și politici.
9. **Rapoarte de testare:** rezultate ale scanărilor de vulnerabilități, testelor de penetrare și revizuirilor de cod.
10. **Ciclul de viață al dezvoltării securizate (SDLC):** politici pentru codare securizată, testare și revizuire, aliniate cu OWASP SAMM sau Microsoft SDL.
11. **Ghid pentru utilizatori:** manuale sau secțiuni de ajutor online care explică funcționalități de securitate cibernetică, precum instalarea actualizărilor și raportarea vulnerabilităților.

4.2 Metodologia de autoevaluare

1. **Listă de verificare a documentației:** verificați prezența tuturor documentelor necesare, inclusiv descrieri ale produsului, evaluări de risc și rapoarte de testare.
2. **Proces de evaluare a riscurilor:** utilizați STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) sau PASTA (Process for Attack Simulation and Threat Analysis) pentru identificarea amenințărilor.
3. **Colectarea dovezilor:** colectați rapoarte de testare, de exemplu Nessus, Metasploit, SBOM-uri și politici SDLC.
4. **Organizarea dosarului tehnic:** utilizați sisteme de management al documentelor precum Confluence, SharePoint sau Notion pentru accesibilitate și pregătire pentru audit.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

5. **Actualizări regulate:** programați revizuiri trimestriale pentru actualizarea documentației, reflectând modificările produsului sau vulnerabilități noi.

Tabel 19 - Model de listă de verificare a documentației

Document	Necesar	Status	Dovezi	Gaps	Action
Descrierea produsului	Da	Complet	Specificație V1.2	None	N/A
Evaluarea riscului	Da	Parțial	Raport STRIDE	Missing mitigation details	Complete by 2025-08-01

4.3 Pași practici pentru IMM-uri

1. **Dezvoltarea descrierii produsului:** detaliați hardware-ul, software-ul, conectivitatea și cazul de utilizare. De exemplu, descrierea unui termostat inteligent include protocoale Wi-Fi și prelucrarea datelor.
2. **Efectuarea evaluării riscurilor:** utilizați STRIDE pentru identificarea amenințărilor precum acces neautorizat sau manipularea datelor. Documentați măsuri de atenuare precum criptarea sau controalele de acces.
3. **Colectarea dovezilor:** compilați rapoarte de testare din instrumente precum Nessus, OWASP ZAP sau SonarQube. Includeți SBOM-uri și politici SDLC.
4. **Organizarea documentației:** utilizați Confluence pentru a crea un dosar tehnic structurat, cu foldere pentru descrieri, evaluări și rapoarte.
5. **Furnizarea ghidului pentru utilizatori:** dezvoltați manuale cu instrucțiuni clare de securitate cibernetică, folosind modele din ETSI EN 303 645.

4.4 Studiu de caz

Un IMM care produce o cameră inteligentă compilează un dosar tehnic:

- **Descriere produs:** detaliază specificațiile camerei, conectivitatea Wi-Fi și stocarea în cloud.
- **Evaluarea riscurilor:** utilizează STRIDE pentru identificarea amenințărilor precum streaming neautorizat, atenuate cu TLS 1.3 și MFA.

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- **Rapoarte de testare:** include rezultatele scanărilor Nessus și rapoarte de testare de penetrare.
- **SDLC:** adoptă OWASP SAMM, documentând practici de codare securizată.
- **Ghid pentru utilizatori:** furnizează un manual cu instrucțiuni de actualizare și o adresă de e-mail CVD.
- **Rezultat:** autoevaluarea verifică exhaustivitatea, identifică lacune în documentația SDLC și planifică remedierea în termen de 6 luni.

4.5 Instrumente și resurse

- **Evaluarea riscurilor:** STRIDE, PASTA, NIST SP 800-30.
- **Testare:** Nessus, OWASP ZAP, Metasploit.
- **Documentare:** Confluence, SharePoint, Notion.
- **Standarde:** OWASP SAMM, Microsoft SDL, ETSI EN 303 645.

Această secțiune asigură că IMM-urile au un dosar tehnic complet, pregătit pentru audit, cu metodologii și modele detaliate.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

5 Procesul de evaluare a conformității și declarația UE de conformitate

Criteriul privind procesul de evaluare a conformității și declarația UE de conformitate finalizează conformitatea CRA, asigurând că IMM-urile urmează modulul de evaluare adecvat și emit o declarație de conformitate validă. Această secțiune oferă o metodologie exhaustivă pentru parcurgerea acestui proces, abordarea obligațiilor post-piață și pregătirea declarației, cu orientări detaliate, modele și studii de caz.

5.1 Module de evaluare a conformității

CRA aplică următoarele module din Anexa VIII:

- **Modul A - Control intern al producției:** producătorul autoevaluează conformitatea cu toate cele 21 de cerințe; menține documentația tehnică și o declarație de conformitate. Este utilizat pentru Default; pentru Clasa I numai în condițiile de la punctul 3.3.
- **Modul B - Examinare UE de tip:** un organism notificat evaluează un „tip" reprezentativ de produs în raport cu cerințele aplicabile.
- **Modul C - Conformitate cu tipul pe baza controlului intern al producției:** producătorul se asigură că producția este conformă cu „tipul" aprobat în Modul B.
- **Modul H - Asigurare completă a calității:** un organism notificat evaluează și monitorizează sistemul complet de calitate al producătorului, proiectare și producție, pentru cerințele aplicabile.

După cum este rezumat la punctul 3.3, aplicarea pentru diferitele clase de produse înseamnă:

- **Default:** Modul A.
- **Important - Clasa I:** Modul A numai dacă sunt aplicate standarde armonizate/specificații comune sau o schemă aplicabilă de certificare UE, nivel cel puțin „substantial"; în caz contrar, B + C sau H.
- **Important - Clasa II:** B + C sau H, ori o schemă aplicabilă de certificare UE, nivel cel puțin „substantial"; Modul A nu este permis.
- **Critic (Anexa IV):** certificare UE obligatorie atunci când este desemnată prin act delegat; până atunci, se urmează art. 32(3), la fel ca pentru Important - Clasa II.

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

5.2 Metodologia de autoevaluare

1. **Determinarea modulului:** identificați modulul necesar pe baza clasificării, Default, Clasa I sau Clasa II.
2. **Efectuarea evaluărilor interne:** pentru Default și Clasa I, verificați conformitatea cu toate cerințele folosind lista de verificare a autoevaluării.
3. **Implicarea organismelor notificate:** pentru Clasa II, transmiteți dosarul tehnic către un organism notificat și abordați constatările auditului.
4. **Abordarea obligațiilor post-piață:** monitorizați vulnerabilitățile, emiteți actualizări și mențineți documentația pe durata ciclului de viață al produsului.
5. **Emiterea declarației:** semnați declarația UE de conformitate, confirmând conformitatea cu cerințele CRA.

Tabel 20 - Model de declarație UE de conformitate

Declarația UE de conformitate
Produs: [Numele produsului] Producător:[Numele companiei, Adresa] Declarăm prin prezenta că produsul de mai sus respectă Regulamentul (UE) 2024/2847 (Actul privind reziliența cibernetică). Cerințe esențiale: Pe deplin conform cu Anexa I. Evaluarea conformității: [Modul, de exemplu, Control intern al producției] Standarde applicate: [de exemplu, ETSI EN 303 645, ISO 27001] Data:[YYYY-MM-DD] Semnătura: Nume, Titulatură

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

5.3 Pași practici pentru IMM-uri

1. **Verificarea clasificării:** confirmați clasa produsului pentru a determina modulul de evaluare.
2. **Efectuarea auditurilor interne:** utilizați lista de verificare a autoevaluării pentru verificarea conformității, susținută de rapoarte de testare și documentație.
3. **Implicarea organismelor notificate:** pentru Clasa II, contactați organisme acreditate, de exemplu prin ENISA, transmiteți dosarul tehnic și pregătiți-vă pentru audituri.
4. **Monitorizarea post-piață:** utilizați instrumente precum Snyk sau NVD al NIST pentru urmărirea vulnerabilităților, emițând patch-uri după caz.
5. **Emiterea declarației:** redactați și semnați declarația de conformitate, incluzând-o în dosarul tehnic.

5.4 Studiu de caz

Un IMM care dezvoltă o jucărie inteligentă de Clasa I efectuează un audit intern, verificând conformitatea cu toate cele 21 de cerințe folosind rapoarte Nessus și OWASP ZAP. Autoevaluarea confirmă exhaustivitatea documentației, conducând la o declarație de conformitate semnată. Pentru un firewall de Clasa II, IMM-ul implică un organism notificat, transmite rapoarte de testare și abordează constatările auditului în termen de 3 luni, documentând procesul.

5.5 Instrumente și resurse

- **Auditare:** Confluence pentru urmărirea auditului, Nessus pentru testare.
- **Organisme notificate:** directorul ENISA.
- **Standarde:** ETSI EN 303 645, ISO 27001.

Această secțiune asigură că IMM-urile finalizează procesul de evaluare a conformității și mențin conformitatea, cu metodologii și modele detaliate.

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Concluzie

Acest cadru metodologic de evaluare a conformității sprijină implementarea de către IMM-uri a Actului UE privind reziliența cibernetică prin orientări aprofundate, exemple practice, studii de caz și instrumente privind cinci criterii-cheie ale CRA: (1) conformitatea cu cerințele esențiale de securitate cibernetică, (2) certificarea produselor cu elemente digitale, (3) clasificarea produselor ca Clasa I sau Clasa II și acțiunile corespunzătoare, (4) exhaustivitatea documentației tehnice și (5) procedurile generale de evaluare a conformității.

În aliniere cu obiectivele proiectului SECURE, ghidul urmărește să facă obligațiile CRA tangibile prin recomandări bazate pe abordări recunoscute și bune practici în domeniul cibernetic, rămânând însă orientativ. Pe baza evoluțiilor viitoare ale contextului juridic al CRA, ghidul poate face obiectul unor modificări. Ca pași următori pentru IMM-uri, se recomandă consultarea ghidurilor suplimentare din repository-ul SECURE, cum ar fi „Cerințele esențiale de securitate cibernetică ale CRA: Anexa I, Partea I" pentru sugestii și recomandări practice pentru fiecare prevedere din Anexa I, precum și „CRA 101: Înțelegerea obligațiilor CRA" pentru o prezentare condensată a obligațiilor legale în temeiul CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE