COMISIA
EUROPEANĂ

Bruxelles, 20.1.2026
COM(2026) 9 final

# RAPORT AL COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

## privind evaluarea Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) și a Cadrului european de certificare a securității cibernetice

{SWD(2026) 2 final}

# 1. INTRODUCERE

## 1.1 Despre ENISA

Înființată în 2004, Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) a urmărit inițial să asigure un nivel ridicat de securitate a rețelelor și a informațiilor în cadrul UE și să cultive o cultură a conștientizării aspectelor legate de securitate în beneficiul părților interesate. De-a lungul anilor, mandatul și responsabilitățile agenției au evoluat semnificativ pentru a ține pasul cu peisajul securității digitale în schimbare rapidă din Europa. Ca răspuns la complexitatea tot mai mare a provocărilor în materie de securitate cibernetică, în 2019, Regulamentul privind securitatea cibernetică a extins mandatul ENISA și i-a acordat un statut permanent în cadrul instituțional al UE. Această extindere a mandatului a consolidat și mai mult rolul ENISA în sprijinirea gestionării și coordonării eforturilor în materie de securitate cibernetică în întreaga UE, punând accentul pe mai multe domenii-cheie:

- acordarea de asistență pentru elaborarea și punerea în aplicare a politicii și legislației UE legate de securitatea cibernetică;
- consolidarea capacității UE de a preveni, detecta și răspunde la incidentele de securitate cibernetică, în special prin furnizarea de asistență operațională și tehnică statelor membre și instituțiilor UE;
- promovarea consolidării capacităților și a cooperării în materie de securitate cibernetică în cadrul UE;
- sensibilizarea publicului, a organizațiilor și a întreprinderilor cu privire la riscurile în materie de securitate cibernetică și promovarea celor mai bune practici;
- contribuția la instituirea și punerea în aplicare a cadrului european de certificare a securității cibernetice, menit să reducă fragmentarea pieței și să consolideze securitatea cibernetică a produselor, serviciilor și proceselor TIC în întreaga UE și
- sprijinirea cooperării cu partenerii internaționali în conformitate cu politicile externe ale UE.

Activitățile ENISA cuprind în prezent recomandări de bază în materie de securitate, rapoarte privind situația amenințărilor, orientări pentru standardizare și studii privind cele mai bune practici în diferite domenii. Agenția organizează ateliere, exerciții și programe de formare pentru a spori expertiza în rândul profesioniștilor din domeniul securității cibernetice și al factorilor de decizie. În plus, ENISA joacă un rol esențial în răspunsul la cererile din partea Comisiei și a statelor membre, în sprijinirea sarcinilor de certificare și în furnizarea de consiliere personalizată cu privire la elaborarea și punerea în aplicare a politicilor în materie de securitate cibernetică.

Impactul preconizat al ENISA include îmbunătățirea securității rețelelor și a informațiilor în cadrul UE, consolidarea încrederii în piața unică digitală și promovarea cooperării în materie de securitate cibernetică între principalele părți interesate din Europa. Pe măsură ce Europa își continuă transformarea digitală, strategiile de adaptare ale ENISA asigură securitatea și reziliența peisajului digital al regiunii, abordând provocări precum amenințările la adresa securității cibernetice, tensiunile geopolitice și fragmentarea politicilor între statele membre.

## 1.2 Despre cadrul european de certificare a securității cibernetice (ECCF)

Cadrul european de certificare a securității cibernetice (ECCF) a fost instituit în temeiul Regulamentului privind securitatea cibernetică, cu scopul principal de a consolida peisajul

securității cibernetice în întreaga Uniune Europeană. ECCF este conceput pentru a crea o abordare unificată și orizontală a certificării securității cibernetice în toate statele membre, reducând astfel fragmentarea în cadrul pieței interne a produselor, serviciilor și proceselor TIC. Astfel, acesta stă la baza încrederii pieței, stimulează creșterea pieței securității cibernetice a UE și asigură o reziliență și capacități solide în materie de securitate cibernetică. Cadrul abordează șase nevoi principale:

- promovarea încrederii pieței la nivelul UE;
- îmbunătățirea măsurilor de securitate cibernetică și a rezilienței;
- stabilirea unor standarde ridicate de reziliență în ofertele de pe piață;
- consolidarea cooperării dintre părțile interesate din domeniul securității cibernetice;
- reducerea sarcinilor de certificare și
- sensibilizarea publicului și a întreprinderilor europene cu privire la securitatea cibernetică.

În plus, ECCF urmărește să sporească transparența în ceea ce privește asigurarea securității cibernetice, promovând securitatea de la stadiul conceperii și securitatea implicită, ceea ce implică atenuarea vulnerabilității și respectarea unor cerințe de securitate specifice.

Pentru a atinge aceste obiective, ECCF se bazează pe mai mulți piloni esențiali, dezvoltarea sistemelor europene de certificare a securității cibernetice fiind esențială pentru aceste eforturi. Cadrul pune accentul pe asigurarea și reziliența cuprinzătoare în materie de securitate cibernetică în întreaga UE prin intermediul acestor sisteme. Cadrul promovează crearea de comunități pentru a oferi contribuții esențiale părților interesate și pentru a facilita cooperarea cu statele membre și între acestea. Regulamentul privind securitatea cibernetică mandatează, de asemenea, o consultare publică a tuturor părților interesate relevante prin intermediul unui proces de consultare formal, deschis, transparent și favorabil incluziunii, precum și formarea de grupuri consultative ad-hoc pentru a colecta diverse perspective și expertiză ca parte a procesului de dezvoltare a sistemului de certificare. ENISA este esențială pentru coordonarea acestor eforturi prin consultarea sistematică a părților interesate pentru a se asigura că toate elementele legislative sunt abordate înainte de a prezenta Comisiei Europene propunerile finale de sisteme în vederea adoptării.

Circumstanțele în materie de securitate cibernetică care stau la baza creării ECCF reflectă o schimbare rapidă a peisajului amenințărilor, acesta fiind marcat de creșterea numărului de atacuri cibernetice care exploatează vulnerabilitățile și de practici de securitate insuficiente, combinate cu fragmentarea emergentă a certificării în UE. Acest peisaj subliniază necesitatea ca misiunea ECCF să asigure integritatea, confidențialitatea și disponibilitatea datelor pe parcursul întregului ciclu de viață al produselor, serviciilor și proceselor TIC. La finalizarea activităților sale de bază, se preconizează că ECCF va produce mai multe realizări, inclusiv documente legate de sisteme, publicații, evenimente și îmbunătățiri structurale care să sprijine punerea în aplicare. Aceste eforturi urmăresc să promoveze o adoptare pe scară mai largă a certificărilor de securitate cibernetică, să raționalizeze procesele, să sporească încrederea pe piața internă și să consolideze atât capacitățile sectorului public, cât și pe cele ale sectorului privat.

Privind în perspectivă, potrivit preconizărilor, contribuțiile ECCF vor consolida reziliența cibernetică și competitivitatea UE, asigurând interacțiuni digitale sigure și fără sincope în cadrul UE și abordând în același timp provocările emergente în materie de securitate cibernetică. Se anticipează efecte majore pe termen mediu și lung, rezultatele favorabile depinzând de factori

interni și externi dinamici, inclusiv de schimbările geopolitice, de evoluția peisajelor de securitate și de nevoile emergente ale pieței.

### 1.3 Scopul raportului

Prezentul raport urmărește să evalueze impactul și eficacitatea ENISA și a ECCF, având în vedere evoluția peisajului tehnologic și de reglementare. În conformitate cu articolul 67 din Regulamentul (UE) 2019/881, cunoscut sub denumirea de „Regulamentul privind securitatea cibernetică", prezenta evaluare nu numai că revizuiește mandatul și activitățile ENISA, ci și evaluează rolul ECCF în promovarea unui mediu cibernetic securizat în întreaga UE până la 28 iunie 2024. Constatările prezentate sunt extrase din raportul de evaluare pregătitor finalizat în decembrie 2024.

Analiza acoperă perioada 2017-2023 și servește mai multor scopuri esențiale. În primul rând, aceasta urmărește să examineze performanța, guvernanța și practicile de lucru ale ENISA și ale ECCF. Acest lucru implică stabilirea gradului în care și-au îndeplinit obiectivele și au contribuit la consolidarea securității cibernetice și a funcționării pieței interne în cadrul UE. Evaluarea se axează pe cinci criterii principale – eficacitatea, eficiența, relevanța, coerența și valoarea adăugată europeană – oferind astfel un cadru pentru înțelegerea realizărilor ambelor entități și a domeniilor în care sunt necesare îmbunătățiri.

Prin examinarea acestor elemente, raportul oferă informații cu privire la posibilele ajustări ale mandatului ENISA și ale strategiilor de consolidare a impactului ECCF. În cele din urmă, aceste evaluări urmăresc să faciliteze luarea unor decizii în cunoștință de cauză pentru a promova reziliența UE în materie de securitate cibernetică. Raportul este structurat în secțiuni distincte: o introducere privind ENISA și ECCF, o analiză a constatărilor evaluării și o sinteză a concluziilor și recomandărilor.

Regulamentul (UE) 2024/2847 (Regulamentul privind reziliența cibernetică) introduce cerințe orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale (hardware și software, inclusiv componentele acestora atunci când sunt introduse pe piață separat). Acesta condiționează introducerea lor pe piața Uniunii de respectarea unui set de cerințe esențiale de securitate cibernetică, urmând abordarea noului cadru legislativ al Uniunii. Regulamentul privind reziliența cibernetică a intrat în vigoare la 10 decembrie 2024 și se va aplica integral de la 11 decembrie 2027. Propunerea Comisiei a fost însoțită de o evaluare cuprinzătoare a impactului, care a analizat motivele care stau la baza introducerii unor astfel de norme. Având în vedere cele de mai sus și faptul că Regulamentul privind reziliența cibernetică se află încă în perioada sa de tranziție, nu s-a considerat necesar să se evalueze în detaliu în prezentul raport al treilea element menționat la articolul 67 alineatul (3) din Regulamentul privind securitatea cibernetică: „Evaluarea examinează dacă sunt necesare cerințe esențiale de securitate cibernetică pentru a avea acces la piața internă, cu scopul de a împiedica ca produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate care nu respectă cerințele de bază în materie de securitate cibernetică să intre pe piața internă."

Întrucât constatările prezentului raport stau la baza obiectivelor de politică ale revizuirii Regulamentului privind securitatea cibernetică, prezentul raport însoțește actul legislativ și, prin urmare, este esențial ca acesta să fie prezentat ca parte a acestui pachet.

## 2. CONSTATĂRILE PRINCIPALE ALE EVALUĂRII

### 2.1 ENISA

Această secțiune prezintă principalele constatări ale evaluării ENISA, concentrându-se asupra eficacității, eficienței, relevanței, coerenței și valorii adăugate pe care o aduce peisajului securității cibernetice din UE. În plus, se oferă o examinare mai atentă a guvernanței interne și a practicilor din cadrul agenției pentru a clarifica dinamica sa operațională și domeniile în care sunt necesare îmbunătățiri.

#### Eficacitate

Raportul de evaluare pregătitor subliniază că ENISA și-a îndeplinit mandatul, obținând aproape toate realizările planificate. Cu toate acestea, trebuie menționat faptul că, în lipsa unor indicatori suficienți, analiza eficacității se bazează în principal pe interviurile și sondajele realizate în rândul părților interesate. În special, în perioade dificile, cum ar fi pandemia de COVID-19 și războiul de agresiune al Rusiei împotriva Ucrainei, agenția a dat dovadă de flexibilitate și a obținut evaluări pozitive din partea părților interesate. În timpul pandemiei de COVID-19, ENISA a sprijinit Comisia și statele membre prin definirea cerințelor de securitate pentru aplicația COVID într-un termen scurt. De asemenea, a jucat un rol în cooperarea cu Ucraina, care a vizat asigurarea faptului că nu există efecte de propagare ale atacurilor asupra infrastructurii și sectoarelor critice, cum ar fi energia. Eficacitatea ENISA rezultă dintr-o structură de guvernanță solidă și dintr-un model organizațional bazat pe o matrice care facilitează îndeplinirea sarcinilor și cooperarea. ENISA și-a atins multe dintre obiective. Părțile interesate au recunoscut și au apreciat, în general, contribuțiile ENISA la consolidarea rezilienței UE în materie de securitate cibernetică. Agenția a promovat cooperarea și schimbul de informații între statele membre și alte părți interesate pentru a sprijini obiectivele UE în materie de securitate cibernetică. Eforturile agenției de a facilita cooperarea tehnică, de a promova standarde comune de securitate cibernetică și de a sprijini inițiativele de consolidare a capacităților au fost deosebit de apreciate. Raportul de evaluare sugerează, de asemenea, că modul de lucru al ENISA poate fi îmbunătățit în ceea ce privește stabilirea priorităților sarcinilor. Prin reevaluarea orientării sale operaționale, ENISA poate valorifica cadrele existente și feedbackul părților interesate pentru a îmbunătăți și mai mult îndeplinirea sarcinilor. Această abordare este deosebit de importantă pentru rezolvarea priorităților emergente, fără a compromite angajamentele existente. Angajamentul continuu al ENISA față de implicarea și consultarea părților interesate a reprezentat un punct forte, însă capacitatea operațională a agenției denotă resurse insuficiente. Utilizarea unei realocări mai dinamice a sarcinilor și a resurselor ar putea contribui parțial la asigurarea îndeplinirii la timp a noilor cereri și la consolidarea capacității ENISA de a răspunde într-o anumită măsură provocărilor în materie de securitate cibernetică. Obiectivul agenției de a-și menține și consolida reputația în comunitatea securității cibernetice ar putea fi realizat în continuare prin asigurarea faptului că sarcinile sunt aliniate nu numai la obiectivele strategice, ci și la capacitatea operațională. Această prioritizare ar trebui facilitată prin eforturi de colaborare între ENISA, statele membre și factorii de decizie de la nivelul UE pentru a asigura alinierea la obiectivele strategice și la capacitatea operațională.

#### Eficiența

În cursul perioadei de evaluare 2017-2023, ENISA a demonstrat că funcționează eficient în cadrul structurii sale de guvernanță existente. Datorită cadrului organizațional bazat pe matrice, ENISA

a acordat prioritate sarcinilor, a optimizat alinierea resurselor și a încurajat cooperarea dintre diferite unități. Această abordare, împreună cu o combinație echilibrată de personal operațional și administrativ, a contribuit la facilitarea îndeplinirii sarcinilor sale mandatate. Cu toate acestea, există o oportunitate clară pentru ENISA de a-și spori eficiența printr-o mai bună stabilire a priorităților, o orientare clară și o alocare mai strategică a resurselor. Eficiența agenției a fost uneori afectată de factori externi și de necesitatea unei guvernanțe interne mai raționalizate. Pe plan intern, ENISA a dezvoltat soluții inovatoare, cum ar fi un model organizațional bazat pe matrice, pentru o coordonare mai eficace între funcțiile operaționale și cele administrative.

Cu toate acestea, evaluarea a evidențiat mai multe domenii-cheie în care ENISA are posibilitatea de a-și îmbunătăți eficiența. Interviurile cu personalul ENISA, sondajele în rândul părților interesate și documentația internă au indicat că agenția a întâmpinat dificultăți în a ține pasul cu cererile tot mai mari și în a ocupa posturi specializate, situație exacerbată de un deficit global de specialiști IT. Acest lucru a dus la întârzieri, la redefinirea priorităților în ceea ce privește sarcinile și la perioade de stres și volum de muncă ridicat. Cu toate acestea, anumite ajustări ar putea atenua aceste provocări. Recentele decizii strategice de realocare a resurselor umane demonstrează o capacitate care poate aborda, într-o anumită măsură, schimbările priorităților. Deși în 2022 a fost pusă în aplicare o creștere bugetară majoră de 15 milioane EUR pentru a integra acțiunea de sprijin în materie de securitate cibernetică, această creștere nu a fost însoțită de o creștere proporțională a personalului. De fapt, o realocare de aproximativ 10,5 ENI în 2022 în vederea adaptării la acțiunea de sprijin în materie de securitate cibernetică demonstrează capacitatea de a optimiza resursele actuale atunci când este necesar, chiar dacă, în acest caz, ENI necesare pentru punerea în aplicare a acțiunii de sprijin au fost, de fapt, obținute parțial prin achiziții publice și parțial prin personal de gestionare a contractelor, astfel cum s-a subliniat în raportul de evaluare pregătitor. Cele 10,5 ENI au fost realocate din programul de lucru existent al agenției, 4 ENI de la activitatea 4 („Facilitarea cooperării operaționale”), 4 ENI de la activitatea 5 („Răspunsul cooperativ la nivelul Uniunii și al statelor membre”) și 2,5 ENI de la alte activități. În consecință, ENISA a luat măsuri pentru a reduce nivelul de prioritate și/sau a reduce anumite activități în 2023, și-a transferat resursele umane către sarcini operaționale care decurg în special din sarcini concrete din legislație, cu efecte secundare negative pentru alte sarcini care erau mai puțin clare din mandatul ENISA, de exemplu în ceea ce privește competențele și sensibilizarea.

Gestiunea bugetară prezintă, de asemenea, oportunități de îmbunătățire. Agenția s-a confruntat cu o tendință descendentă în ceea ce privește echilibrarea creditelor aprobate și a celor angajate între 2019 și 2022 din cauza întârzierilor înregistrate în cadrul unor acțiuni precum acțiunea de sprijin în materie de securitate cibernetică. Prin inversarea acestei tendințe și prin eforturile depuse în direcția gestionării cheltuielilor administrative, inclusiv prin abordarea întârzierilor în materie de achiziții publice, eficiența internă ar putea fi îmbunătățită într-o mai mare măsură.

**Relevanța**

Relevanța ENISA în domeniul securității cibernetice este subliniată de capacitatea sa de reacție la evoluția nevoilor părților interesate și de flexibilitatea sa de a se adapta la peisajul în schimbare. Agenția și-a demonstrat în mod constant capacitatea de a-și revizui și de a-și realinia domeniile de acțiune pentru a aborda evoluțiile emergente, menținându-și astfel poziția de componentă vitală în cadrul de securitate cibernetică al UE. Deși nivelul de satisfacție al părților interesate cu privire la eforturile ENISA este, în general, pozitiv, există dimensiuni în care relevanța acesteia poate fi sporită în continuare. În pofida caracterului său reactiv, ENISA ar putea îmbunătăți sprijinul și ar

putea spori vizibilitatea în rândul diferitelor sectoare și părți interesate, în special pentru IMM-uri, care adesea întâmpină dificultăți în a îndeplini cerințele în materie de securitate cibernetică. Trecerea la furnizarea unor instrumente și resurse mai directe, adaptate la sectoare specifice, dar care să ofere, de asemenea, informații și instrumente pentru a aborda amenințările emergente poate spori impactul agenției. Abordarea agenției în ceea ce privește implicarea părților interesate a fost eficace, utilizând forumuri, comitete și grupuri de lucru pentru a implica în mod activ experții naționali în operațiuni și publicații. Cu toate acestea, structura descentralizată complexă din unele state membre a generat provocări care ar putea fi atenuate printr-o mai bună organizare și o coordonare mai clară cu autoritățile naționale. Inițiativele în curs ale agenției, inclusiv elaborarea de orientări în materie de securitate cibernetică și de programe de consolidare a capacităților, reflectă angajamentul său de a promova cooperarea și de a consolida poziția colectivă a UE în materie de securitate cibernetică. Promovarea unei colaborări mai strânse între industrii și îmbunătățirea accesului la informații ar putea aborda unele limitări percepute de sectorul industrial. Potențialul considerabil de îmbunătățire al ENISA constă în reevaluarea priorităților, raționalizarea proceselor și dobândirea de noi resurse adecvate și maximizarea eficientă a resurselor existente, consolidând astfel rolul său fundamental în ecosistemul de securitate cibernetică al Europei. Prin alinierea strategică la Strategia europeană de securitate cibernetică, prioritățile revizuite ale ENISA ar putea crea căi pentru contribuții cu un impact mai mare. Consolidarea capacității agenției de a oferi sprijin politic și tehnic ar putea implica furnizarea mai multor resurse și o mai mare selectivitate în ceea ce privește angajamentele sale și îmbunătățirea domeniilor sale de interes operațional. În concluzie, deși relevanța ENISA este clară, se mai pot aduce îmbunătățiri. Prin redefinirea priorităților activităților și prin furnizarea mai multor resurse și optimizarea resurselor existente, ENISA își poate consolida atât eficiența, cât și impactul global, aliniindu-se mai îndeaproape la cerințele dinamice ale peisajului european al securității cibernetice.

**Coerența**

În evaluarea coerenței ENISA, evaluarea evidențiază atât punctele forte, cât și domeniile în care sunt necesare îmbunătățiri. Angajamentul ENISA de a promova cooperarea în materie de securitate cibernetică la nivelul UE este evident, în special prin facilitarea acesteia și prin colaborarea directă cu părțile interesate. Această abordare dublă a permis ENISA să contribuie în mod semnificativ la domeniul cibernetic, aliniindu-se la cadrele legislative recente. Cu toate acestea, deși rolul ENISA de facilitator și coordonator este pozitiv, mai multe domenii necesită îmbunătățiri pentru a spori coerența. Evaluarea a identificat necesitatea de a îmbunătăți sinergiile dintre responsabilitățile și acțiunile ENISA și cele ale altor organisme ale UE, cum ar fi Centrul european de competențe în materie de securitate cibernetică (ECCC), precum și ale autorităților naționale din domeniul securității cibernetice. Deși aceste roluri sunt adesea complementare, există oportunități de a raționaliza și mai mult operațiunile și de a îmbunătăți eficiența organizațională. Prin oficializarea acordurilor de cooperare cu alte entități, cum ar fi EMSA și JRC, ENISA ar putea valorifica mai bine sinergiile și ar putea asigura o abordare unificată a inițiativelor în materie de securitate cibernetică. Comunicarea internă și gestionarea resurselor în cadrul ENISA ar trebui, de asemenea, îmbunătățite. Interacțiunea agenției cu părțile interesate din sectorul privat și cu partenerii internaționali trebuie să fie mai previzibilă și mai transparentă pentru a menține încrederea și a încuraja eforturile de colaborare. În conformitate cu Regulamentul privind reziliența cibernetică și cu Directiva NIS 2, o delimitare clară a sarcinilor ENISA în ceea ce privește sprijinul pentru punerea în aplicare a politicilor ar putea spori eficiența și ar putea asigura coerența între măsurile de reglementare. Această claritate ar îmbunătăți, de asemenea, capacitatea ENISA de a răspunde

cerințelor de reglementare sectoriale. Pe scurt, deși ENISA a demonstrat o bază solidă în promovarea coerenței în materie de securitate cibernetică în UE, agenția are posibilitatea de a-și redefini prioritățile în ceea ce privește eforturile. Această abordare o va ajuta să își îndeplinească mandatul în mod eficient și să se adapteze la peisajul în continuă evoluție al securității cibernetice. Prin abordarea ineficiențelor actuale și prin consolidarea coordonării între agenții, ENISA își poate menține în mod eficace rolul esențial în cadrul de securitate cibernetică al UE.

**Valoarea adăugată a UE**

ENISA a contribuit în mod semnificativ la consolidarea ecosistemului de securitate cibernetică al UE, însă există oportunități de îmbunătățire care ar putea amplifica impactul acesteia. Servind drept nod centralizat, ENISA a facilitat cooperarea vitală în întreaga UE, a completat eforturile naționale, în special în statele membre cu infrastructuri de securitate cibernetică mai puțin dezvoltate, și a aliniat practicile și politicile în materie de securitate cibernetică. În calitate de agenție descentralizată a UE, mandatul specializat al ENISA i-a permis să își consolideze expertiza în materie de securitate cibernetică și să colaboreze în mod eficace cu statele membre, jucând un rol esențial în modelarea peisajului securității cibernetice din Europa. În acest context, este esențial ca ENISA să se concentreze asupra statelor membre, având în vedere rolul său în furnizarea de informații cu privire la amenințările emergente și în recomandarea de instrumente și strategii pentru abordarea acestora. Agenția ar putea consolida și mai mult cooperarea internațională, în conformitate cu prioritățile Uniunii, inclusiv cu partenerii din țări terțe, cu organizațiile internaționale și cu agențiile de securitate cibernetică, pentru a aborda mai bine natura globală a amenințărilor cibernetice. În plus, ENISA joacă un rol esențial în promovarea certificării securității cibernetice și în sprijinirea activităților de standardizare, ceea ce contribuie la reducerea fragmentării pieței și promovează practici solide în materie de securitate cibernetică în întreaga UE. În pofida absenței unor organisme similare cu expertiza și agilitatea organizațională a ENISA, accentul principal pe care aceasta îl pune în prezent pe autoritățile naționale a atras critici din partea părților interesate din sectorul privat. Feedbackul din partea actorilor importanți din industrie indică faptul că s-ar putea face mai mult pentru a adapta informațiile la provocările specifice ale sectorului privat. Deși accentul principal pus pe autoritățile naționale este esențial, consolidarea strategică a implicării părților interesate și a colaborării cu industria ar putea răspunde acestor preocupări. În plus, mandatul ENISA ar putea beneficia de pe urma reevaluării strategice a priorităților sale pentru a se adapta fără probleme la provocările în continuă evoluție în materie de securitate cibernetică. Acest lucru ar permite ENISA să își mențină contribuțiile valoroase la UE, abordând în același timp în mod eficace nevoile tot mai mari ale diferitelor părți interesate.

**Principalele realizări și provocări**

ENISA este recunoscută pe scară largă în cadrul comunității de securitate cibernetică a UE pentru reputația sa solidă, pentru publicațiile de calitate și pentru rolul său semnificativ în promovarea cooperării dintre statele membre și alte entități de securitate cibernetică. Activitatea ENISA care contribuie la armonizarea cerințelor în materie de securitate cibernetică este esențială pentru stabilirea unui nivel coerent de protecție în toate statele membre, contribuind în mod direct la consolidarea capacităților, în special pentru statele membre mai mici. Această armonizare nu numai că asigură un mediu digital sigur în întreaga UE, ci și sporește gradul de pregătire în materie de securitate cibernetică în rândul părților interesate.

Cu toate acestea, evaluarea a identificat mai multe provocări cu care se confruntă ENISA. ENISA are o agilitate limitată în ceea ce privește răspunsul la amenințările în continuă evoluție la adresa securității cibernetice, ceea ce poate duce la posibile întârzieri în activitățile sale. Pentru a atenua provocările legate de constrângerile în materie de resurse, părțile interesate consultate[2] au subliniat, printre altele, necesitatea îmbunătățirii proceselor de recrutare și a strategiilor de gestionare a volumului de muncă. Extinderea mandatului ENISA pentru a consolida rolul său operațional ar putea răspunde acestor preocupări, permițându-i să valorifice progresele tehnologice și să îmbunătățească cadrele de securitate cibernetică. Această restructurare ar permite ENISA să abordeze în mod proactiv amenințările dinamice, sporind impactul acesteia prin inițiative comune de formare și prin contribuții la procesele de elaborare a politicilor.

În cele din urmă, sistemele ENISA de consultare și gestionare a părților interesate sunt considerate eficace în facilitarea gestionării nevoilor și așteptărilor părților interesate, însă este necesară o relație mai puternică și mai transparentă cu statele membre pentru a consolida cooperarea și schimbul de informații. Printre prioritățile viitoare se numără actualizarea cadrelor interne pentru a gestiona mai bine responsabilitățile tot mai mari și diferitele provocări, asigurându-se că ENISA își poate îndeplini pe deplin sarcinile care îi revin, având în vedere numărul său de angajați.

## 2.2 ECCF

Această secțiune prezintă principalele constatări ale evaluării privind ECCF, concentrându-se asupra eficacității, eficienței, relevanței, coerenței și valorii adăugate pe care o aduce peisajului securității cibernetice din UE. În plus, raportul sintetizează principalele puncte forte și puncte slabe identificate ale cadrului, pe baza unei analize SWOT.

### Eficacitatea

ECCF a fost conceput ca un pilon pentru îmbunătățirea asigurării securității cibernetice pe piața internă a UE, cu scopul de a armoniza certificarea produselor, serviciilor și proceselor TIC. Acesta a fost instituit pentru a aborda aspecte persistente, cum ar fi fragmentarea pieței și necesitatea unei transparențe sporite și a unei încrederi sporite a publicului în soluțiile digitale. Prin modelul său structurat de guvernanță care implică entități precum ENISA, Grupul european pentru certificarea securității cibernetice (ECCG) și Rețeaua autorităților naționale de certificare a securității cibernetice, ECCF a pus bazele unei coordonări sporite între părțile interesate, inclusiv statele membre și entitățile private. Cu toate acestea, realizarea practică a acestor obiective s-a confruntat cu numeroase provocări care au limitat eficacitatea ECCF. O deficiență semnificativă a actualului ECCF este incapacitatea sa de a aborda în mod eficace fragmentarea sistemelor de certificare în întreaga UE, în principal din cauza limitărilor procedurale. Această fragmentare a persistat în pofida intenției cadrului de a armoniza procesele de certificare, ceea ce a condus la inconsecvențe și ineficiență în asigurarea securității cibernetice. Acest lucru se poate observa în întârzierea substanțială în operaționalizarea primului sistem de certificare, criteriile comune ale UE (EUCC), care a durat 57 de luni de la inițiere până la adoptare. Această întârziere evidențiază ineficiența proceselor cadrului, influențată în principal de procedurile de aprobare complexe și multidimensionale. În plus, ambiguitatea în ceea ce privește responsabilitățile și răspunderea în rândul părților interesate a complicat și mai mult capacitatea cadrului de a-și atinge obiectivele. Factorii externi au complicat și mai mult obiectivele ECCF. Peisajul geopolitic în continuă evoluție, caracterizat de creșterea amenințărilor cibernetice și a tensiunilor politice legate de

suveranitatea datelor și de controlul digital, a necesitat măsuri de adaptare, iar ECCF a întâmpinat dificultăți în a le pune în aplicare rapid. Aceste presiuni externe au dus la adoptarea cu întârziere a sistemelor, astfel cum s-a observat în cazul EUCS (sistemul european de certificare domeniul cloud computingului), unde discuțiile au stagnat în cadrul dezbaterilor fără caracter tehnic, cum ar fi cerințele de localizare a datelor. În pofida acestor obstacole, au existat rezultate pozitive – în special în ceea ce privește sensibilizarea statelor membre cu privire la importanța și complexitatea certificării securității cibernetice. Deși a cauzat întârzieri operaționale, pandemia de COVID-19 a subliniat, de asemenea, necesitatea unei infrastructuri digitale reziliente, punând securitatea cibernetică în centrul atenției în materie de politici. Pandemia de COVID-19 a avut influențe atât negative, cât și pozitive asupra ECCF. În ceea ce privește aspectele „negative", tranziția bruscă către reuniunile online a contribuit la întârzierea proceselor de dezvoltare a sistemului. În ceea ce privește aspectele „pozitive", pandemia de COVID-19 a sporit gradul de conștientizare cu privire la importanța lanțurilor de aprovizionare reziliente care depind mai puțin de țări terțe. În plus, analiza a identificat învățăminte esențiale, remarcând alocarea inegală a resurselor între părțile interesate, inclusiv între statele membre, ceea ce împiedică dezvoltarea și punerea în aplicare uniformă a sistemelor de certificare. Abordarea acestor disparități este vitală pentru eficiența și eficacitatea viitoare, în special prin păstrarea personalului de specialitate în cadrul ENISA și prin promovarea unui dialog constant între toate părțile implicate.

**Eficiența**

Eficiența ECCF a făcut obiectul unei examinări, având în vedere termenele extinse pentru adoptarea sistemelor de certificare a securității cibernetice și multitudinea aspectelor complexe implicate. În pofida intenției sale strategice de a raționaliza procesul de certificare în întreaga UE, eficiența ECCF a fost afectată în special de discuțiile și etapele de pregătire elaborate, care au culminat cu întârzieri semnificative; primul sistem a fost adoptat abia la începutul anului 2024, la aproape cinci ani de la punerea în aplicare. Aceste termene prelungite pot fi atribuite unor provocări multidimensionale, care includ atât dimensiunea politică, cât și cea tehnică.

Provocările politice, inclusiv politizarea discuțiilor privind cerințele de certificare, au împiedicat realizarea de progrese prin crearea unui mediu în care transparența și comunicarea au avut de suferit. De exemplu, sistemul UE de certificare în domeniul cloud computingului (EUCS) a fost afectat în mod semnificativ de dezbaterile privind cerințele de suveranitate a datelor, atrăgând presiuni politice din partea țărilor terțe și a industriei din afara UE, ceea ce a condus la trecerea de la discursul tehnic la cel politic în cadrul ECCG.

Complexitatea tehnică a contribuit și mai mult la ineficiențe, în special la dificultatea de a transpune proiectele de sisteme în acte juridice, având în vedere natura diversă și exigența produselor/serviciilor destinate certificării, cum ar fi tehnologia 5G și cloud computingul. Numeroasele solicitări și lipsa unor standarde stabilite în anumite domenii au adăugat niveluri de dificultate proceselor de pregătire și adoptare, impunând unui număr mare de părți interesate să asigure alinierea la politicile și practicile existente în multe etape. În pofida acestor cazuri de ineficiență, în acest cadru au apărut mai multe elemente pozitive. Crearea unor grupuri și forumuri dedicate, inclusiv a Grupului european pentru certificarea securității cibernetice (ECCG), a Grupului de lucru ad-hoc dedicat sistemelor specifice și a Grupului părților interesate pentru certificarea securității cibernetice (SCCG), a facilitat implicarea necesară a părților interesate. Cu toate acestea, se mai pot aduce îmbunătățiri substanțiale în ceea ce privește asigurarea unei funcționări optime a acestor structuri; de exemplu, membrii SCCG au perceput o lipsă de implicare

a grupului în ECCF. Îmbunătățirea guvernanței interne este esențială pentru a aborda participarea activă și contribuția strategică a părților interesate.

**Relevanța**

ECCF apare ca un răspuns esențial la caracterul din ce în ce mai complex și sofisticat al amenințărilor cibernetice în întreaga UE, urmărind să instituie sisteme armonizate de certificare a securității cibernetice care să asigure încrederea și să promoveze o piață digitală sigură. În pofida premisei sale promițătoare, se consideră în continuare că relevanța cadrului este mai mult potențială decât practică, sistemele de certificare intrând abia recent în faza operațională. Această realizare întârziată a rezultatelor tangibile subliniază disparitățile în materie de execuție și generează incertitudine cu privire la poziția actuală a ECCF în peisajul securității cibernetice. Importanța ECCF rezidă în rolul său strategic în creșterea standardelor de securitate cibernetică și în facilitarea recunoașterii reciproce a certificărilor în toate statele membre, reducând astfel costurile individuale ale întreprinderilor și îmbunătățind funcționarea pieței interne. Cadrul urmărește o integrare solidă cu alte acte juridice ale UE, cu scopul de a raționaliza procedurile și de a facilita comerțul transfrontalier.

Mai mulți factori consolidează relevanța ECCF, în pofida provocărilor cu care se confruntă în îndeplinirea sarcinilor sale. Creșterea bruscă a amenințărilor cibernetice sporește considerabil necesitatea unei strategii unitare de securitate cibernetică care să se poată adapta rapid la scenarii în schimbare, cum ar fi relevanța sporită a certificării în domenii care necesită un nivel înalt de asigurare, cum ar fi serviciile de cloud și infrastructurile 5G. Mandatele de achiziții publice din aceste sectoare reflectă cererea tot mai mare pentru un cadru de certificare unificat și fiabil, o cerere pe care ECCF o poate îndeplini. În plus, legătura ECCF cu actele legislative emergente, în special cu Regulamentul privind reziliența cibernetică și cu Directiva NIS 2 (Securitatea rețelelor și a informațiilor), evidențiază valoarea sa anticipată în abordarea nevoilor în materie de infrastructură critică și a conformității juridice în întreaga UE. Rolul proactiv al ENISA și instituirea autorităților naționale de certificare a securității cibernetice marchează etape esențiale în direcția consolidării interacțiunilor colaborative și a promovării adoptării certificării. Cu toate acestea, decalajele în ceea ce privește alocarea resurselor și expertiza între statele membre mai mari și cele mai mici continuă să perpetueze dezechilibrele în ceea ce privește participarea și eficacitatea, afectând dezvoltarea sistemelor colective.

**Coerența**

Coerența ECCF este, de asemenea, afectată de lipsa unor mecanisme clare de răspundere, ceea ce a condus la dificultăți în alinierea obiectivelor sale la alte măsuri legislative. Această neconcordanță riscă să creeze suprapuneri și ineficiențe în peisajul securității cibernetice. Coerența deplină a ECCF cu alte instrumente legislative ale UE, inclusiv cu Directiva NIS 2 și cu Regulamentul privind reziliența cibernetică, este esențială pentru asigurarea unei abordări unificate în materie de securitate cibernetică. ECCF prezintă o aliniere teoretică la aceste măsuri legislative, concepute pentru a aborda diferite aspecte ale securității cibernetice în peisajul UE, însă integrarea în lumea reală rămâne complexă și necesită o supraveghere atentă. Viitoarea punere în aplicare a sistemului de criterii comune ale UE (EUCC) reprezintă un test semnificativ pentru această coerență, deoarece implementarea sa cu succes va demonstra capacitatea ECCF de a armoniza și de a mobiliza în mod eficace eforturi legislative suplimentare. Părțile interesate au subliniat necesitatea unei coordonări atente între ECCF și actele de reglementare emergente pentru a preveni

suprapunerile, care ar putea submina eficiența și ar putea dilua impactul preconizat în toate sectoarele. Mai precis, apar preocupări cu privire la interfața dintre ECCF și Regulamentul privind reziliența cibernetică, întrucât ambele inițiative vizează consolidarea standardelor de securitate cibernetică, dar riscă să fie redundante dacă nu sunt aplicate într-o sinergie completă, în care o legislație o sprijină și o completează pe cealaltă. În ceea ce privește sectorul, coerența trebuie extinsă pentru a ține seama de progresele tehnologice continue, asigurându-se că inițiativele în materie de securitate cibernetică sunt nuanțate în mod corespunzător pentru a răspunde nevoilor în materie de infrastructură critică.

**Valoarea adăugată a UE**

În pofida potențialului său, ECCF a întâmpinat dificultăți în a aduce valoare adăugată prin promovarea unui mediu unificat și eficace în materie de securitate cibernetică în întreaga UE. ECCF a urmărit să consolideze în mod semnificativ peisajul securității cibernetice din UE prin introducerea unei proceduri de dezvoltare și a unei structuri de guvernanță fără precedent pentru procesele de certificare. În esență, ECCF a reprezentat un progres esențial în ceea ce privește capacitatea UE de a crea o abordare armonizată a certificării produselor, serviciilor și proceselor TIC. Valoarea adăugată inerentă a acestui cadru la nivelul UE constă în potențialul său de a elimina abordările naționale disparate, promovând o piață internă cu standarde de securitate cibernetică coerente, fiabile și recunoscute în toate statele membre. Cu toate acestea, termenele prelungite și punerea în aplicare fragmentată a sistemelor au împiedicat capacitatea ECCF de a-și valorifica pe deplin valoarea preconizată. Mai precis, întârzierea sistemelor care pot fi puse în aplicare, evidențiată de adoptarea tardivă a unor inițiative precum criteriile comune ale UE (EUCC), a redus impactul imediat, lăsând în mare măsură neatins potențialul său teoretic. Disparitățile în ceea ce privește punerea în aplicare sistemică, agravate de grade diferite de pregătire și de disponibilitate a resurselor între statele membre, diluează și mai mult influența cuprinzătoare a cadrului. Cu toate acestea, ECCF a revigorat dinamica de cooperare în întreaga UE. Prin înființarea unor grupuri precum ECCG, acesta a instituționalizat eforturile de coordonare, permițând o implicare mai amplă la diferite niveluri de guvernanță. Această infrastructură colaborativă încurajează schimbul de informații și strategiile comune, promovând o poziție unificată în materie de securitate cibernetică împotriva amenințărilor în continuă evoluție. Pentru ca ECCF să își deblocheze întreaga valoare adăugată europeană, este esențială o participare sporită și concisă a părților interesate. Promovarea unui mediu favorabil incluziunii, în care partenerii din sector, autoritățile naționale și organismele UE să contribuie în mod activ la procesul de certificare și să îl ghideze, va asigura acceptarea pe scară largă și eficacitatea standardelor de securitate cibernetică.

**Principalele realizări și provocări**

ECCF servește drept instrument esențial pentru consolidarea colaborării la nivelul UE între ENISA, statele membre și sectoare, consolidând relevanța acestuia în mediul dinamic al securității cibernetice. Adaptabilitatea sa facilitează dezvoltarea sistemului prin intermediul grupurilor de lucru ad-hoc și se aliniază la cadrele legislative ale UE, cum ar fi NIS2. Deși semnificativ, acest potențial rămâne în mare măsură neexploatat din cauza punerii în aplicare limitate a sistemelor efective.

ECCF este esențial pentru abordarea amenințărilor emergente la adresa securității cibernetice și pentru promovarea conformității, în special în ceea ce privește valorificarea noilor tehnologii, cum ar fi inteligența artificială. Părțile interesate recunosc rolul său în consolidarea cooperării dintre

statele membre și în îmbunătățirea pregătirii în materie de securitate cibernetică. Valoarea sa în promovarea schimburilor pe piața internă, prin înlocuirea sistemelor naționale de certificare cu sisteme la nivelul UE, este, de asemenea, recunoscută.

Cu toate acestea, ECCF este afectat de deficiențe semnificative. Procesele îndelungate de adoptare a sistemelor îi afectează eficacitatea, o provocare exacerbată de complexitatea tehnică și de presiunile politice exercitate de activitățile de lobby din industrie. Aceste întârzieri subminează încrederea și împiedică adoptarea rapidă a sistemelor europene de certificare a securității cibernetice. Există oportunități pentru ECCF de a consolida cadrele de securitate cibernetică ale UE, însă amenințări precum constrângerile în materie de resurse și tensiunile geopolitice reprezintă provocări. Modificările priorităților de politică și potențialele suprapuneri legislative ar putea afecta eficacitatea cadrului, riscând inconsecvențe pe piață. Abordarea acestor aspecte este vitală pentru a asigura evoluția ECCF de la un concept promițător la un mecanism pe deplin operațional, consolidând standardizarea și certificarea securității cibernetice la nivelul UE.

## 3. CONCLUZII ȘI RECOMANDĂRI

### 3.1 ENISA

Evaluarea ENISA subliniază rolul său esențial în eforturile de creare a unui peisaj coerent în materie de securitate cibernetică în întreaga UE. ENISA și-a demonstrat eficacitatea și a generat rezultate valoroase. Întrucât cererile adresate ENISA continuă să crească, este important să se reevalueze și să se raționalizeze operațiunile acesteia pentru a alinia mai bine resursele și prioritățile, cu un accent continuu pe sprijinirea statelor membre în abordarea amenințărilor la adresa securității cibernetice și pe consolidarea infrastructurilor naționale de securitate cibernetică. Perfecționarea procesului său de elaborare a rapoartelor, făcându-le mai ușor de utilizat și mai accesibile prin mijloace vizuale și rezumate concise, ar putea spori eficacitatea și relevanța ENISA în peisajul actual al amenințărilor. Consolidarea canalelor de comunicare este esențială pentru a se asigura că activitățile și serviciile ENISA sunt vizibile în mod clar pentru părțile interesate, inclusiv pentru actorii din industrie. O strategie de comunicare bine definită ar putea contribui la promovarea unor conexiuni și a unei cooperări mai strânse în cadrul rețelelor de securitate cibernetică existente, cum ar fi ISAC.

ENISA își poate îmbunătăți eficiența punând un accent mai strategic pe stabilirea priorității sarcinilor, permițând o abordare mai raționalizată a gestionării presiunilor legate de volumul de muncă. Pentru a îmbunătăți relevanța în rândul părților interesate, rolul central al ENISA în sprijinirea statelor membre ar trebui să fie consolidat în continuare prin consolidarea capacității sale de a oferi informații în timp util cu privire la amenințările emergente și la instrumentele strategice pentru abordarea acestora. În plus, astfel cum au indicat o serie de părți interesate, ENISA ar putea stabili metode mai structurate și mai transparente de colaborare cu entități private, inclusiv de sprijinire a IMM-urilor. Ar trebui urmărită claritatea în ceea ce privește rolul ENISA în punerea în aplicare a politicilor împreună cu alte instituții ale UE, asigurându-se că în avangarda acestor eforturi de consolidare a coeziunii strategiei unificate de securitate cibernetică a UE se află colaborarea cu statele membre, care ar include, de asemenea, consolidarea cooperării cu alte agenții ale UE și căutarea de sinergii cu alte organisme de securitate cibernetică pentru acțiuni comune de sporire a coerenței operaționale în întreaga Europă.

În general, este importantă menținerea statutului ENISA ca agenție specializată în cadrul UE, deoarece asigură un accent continuu pe prioritățile în materie de securitate cibernetică. Aceste recomandări urmăresc să consolideze capacitatea ENISA de a-și gestiona în mod eficace responsabilitățile și să reafirme rolul său de entitate principală în domeniul securității cibernetice.

### 3.2 ECCF

Evaluarea ECCF evidențiază mai multe recomandări strategice. În primul rând, în pofida rolului esențial al ENISA în promovarea cooperării și a coeziunii operaționale între statele membre și alte părți interesate, constrângerile privind eficiența și eficacitatea ECCF au fost evidente, în principal din cauza complexității proceselor de adoptare a sistemelor. Aceste aspecte evidențiază necesitatea unei revizuiri substanțiale a structurilor de guvernanță pentru a spori claritatea operațională și responsabilitatea la toate nivelurile.

Pentru a aborda aceste constatări, se recomandă mai multe acțiuni de optimizare a contribuției ENISA la ECCF. Ar trebui să existe un efort concertat pentru a asigura o distribuție coerentă și adecvată a resurselor financiare și umane între ENISA și alte părți interesate din cadrul ECCF. Stabilizarea regimurilor de ocupare a forței de muncă este esențială pentru a reduce fluctuația și a consolida memoria instituțională, facilitând astfel punerea în aplicare eficientă a sistemelor și întreținerea continuă. Dezvoltarea unor procese decizionale raționalizate în cadrul ECCF, care să clarifice rolurile și responsabilitățile, va promova transparența și eficiența, în special în ceea ce privește consolidarea eforturilor de colaborare între statele membre, Comisie și ENISA. Acest lucru va promova responsabilitatea și va reduce ineficiențele. Este esențial un angajament de stabilire și respectare a unor termene realiste pentru dezvoltarea și punerea în aplicare a sistemelor de certificare. Acest lucru implică sprijinirea unei analize tehnice detaliate și consolidarea eforturilor de pregătire pentru a anticipa și a atenua în mod eficace influențele politice.

În plus, investițiile active în formarea și păstrarea personalului calificat în cadrul ENISA sunt esențiale pentru a asigura continuitatea și expertiza atunci când se confruntă cu provocări complexe în materie de securitate cibernetică. Stabilitatea pe termen lung a forței de muncă va fi vitală pentru menținerea eficacității operaționale a ECCF. În plus, ar trebui sporită sensibilizarea industriei și a consumatorilor prin campanii specifice și implicare strategică, subliniind valoarea produselor și a serviciilor certificate. O abordare proactivă în ceea ce privește obținerea de sprijin din partea părților interesate este esențială pentru stimularea cererii și a încrederii în inițiativele ECCF.