Consiliul
Uniunii Europene

Bruxelles, 22 ianuarie 2026
(OR. en)

5611/26

Dosar interinstituțional:
2026/0011 (COD)

CYBER 29
JAI 85
DATAPROTECT 22
TELECOM 29
MI 58
IND 48
CADREFIN 26
FIN 100
BUDGET 3
CODEC 90

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	21 ianuarie 2026
Destinatar:	Dna Thérèse BLANCHET, Secretară Generală a Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2026) 11 final
Subiect:	Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI privind Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), cadrul european de certificare a securității cibernetice și securitatea lanțului de aprovizionare TIC și de abrogare a Regulamentului (UE) 2019/881 (Regulamentul privind securitatea cibernetică 2)

În anexă, se pune la dispoziția delegațiilor documentul COM(2026) 11 final.

Anexă: COM(2026) 11 final

COMISIA
EUROPEANĂ

Strasbourg, 20.1.2026
COM(2026) 11 final

2026/0011 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), cadrul european de certificare a securității cibernetice și securitatea lanțului de aprovizionare TIC și de abrogare a Regulamentului (UE) 2019/881 (Regulamentul privind securitatea cibernetică 2)

{SEC(2026) 11 final} - {SWD(2026) 11 final} - {SWD(2026) 12 final}

(Text cu relevanță pentru SEE)

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

• Motivele și obiectivele propunerii

De la adoptarea Regulamentului privind securitatea cibernetică în 2019, peisajul amenințărilor la adresa securității cibernetice a evoluat semnificativ[1] într-o realitate geopolitică din ce în ce mai complexă. Atacurile cibernetice s-au intensificat și au devenit mai sofisticate, vizând infrastructura critică, întreprinderile și publicul larg, în centrul acestora aflându-se activitatea de tip ransomware[2]. Tehnologiile emergente, cum ar fi inteligența artificială (IA) și informatica cuantică, remodelează instrumentele de apărare și tacticile adversarilor. În raportul său din 2024 intitulat **„Viitorul competitivității europene”**, Mario Draghi a subliniat necesitatea de a spori securitatea și de a reduce dependențele ca unul dintre principalele domenii de acțiune necesare în Uniunea Europeană[3]. Atât Strategia europeană privind o Uniune a pregătirii[4], cât și Strategia europeană de securitate internă (ProtectEU)[5] au plasat securitatea cibernetică în centrul agendei Uniunii privind reziliența. Aceste strategii recunosc că amenințările persistente la adresa securității cibernetice nu sunt doar provocări tehnice, ci și riscuri strategice pentru democrația, economia și modul nostru de viață. În mod similar, Comunicarea privind consolidarea securității economice a UE[6] identifică drept obiective prioritare prevenirea accesului la informații și date sensibile care ar putea submina securitatea economică a Uniunii și prevenirea și atenuarea perturbărilor infrastructurii critice a Uniunii care afectează economia Uniunii, iar în cadrul acestora măsurile eficace de securitate cibernetică joacă un rol esențial.

În acest context, **există patru probleme principale** pe care prezenta propunere de revizuire a Regulamentului privind securitatea cibernetică urmărește să le abordeze: (i) neconcordanța dintre cadrul de politică al Uniunii în materie de securitate cibernetică și nevoile părților interesate într-un peisaj al amenințărilor din ce în ce mai ostil; (ii) stagnarea punerii în aplicare a cadrului european de certificare a securității cibernetice (ECCF); (iii) complexitatea și diversitatea politicilor legate de securitatea cibernetică care au un impact asupra posturii de securitate cibernetică a Uniunii și (iv) creșterea riscurilor la adresa securității lanțurilor de aprovizionare TIC.

Pe baza principalelor probleme identificate, **cele două obiective generale** ale intervenției sunt de a spori capacitățile și reziliența în materie de securitate cibernetică și de a preveni fragmentarea pe piața unică prin:

- contribuția la consolidarea guvernanței Uniunii în materie de securitate cibernetică și contribuția la asigurarea faptului că instituțiile, autoritățile și alte părți interesate

---

1 ENISA, *ENISA Threat Landscape 2024* (Raportul privind situația amenințărilor pentru 2024), https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

2 ENISA, *ENISA Threat Landscape 2025* (Raportul privind situația amenințărilor pentru 2025).

3 Comisia Europeană, Viitorul competitivității europene, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf.

4 JOIN(2025) 130 final.

5 COM(2025) 148 final.

6 JOIN(2025) 977 final.

relevante sunt mai bine pregătite pentru a preveni, a detecta amenințările la adresa securității cibernetice și a răspunde la acestea într-un mod coordonat și eficace și

- sprijinirea dezvoltării, a punerii în aplicare și a adoptării unor instrumente comune ale Uniunii în materie de securitate cibernetică, cum ar fi sistemele de certificare, și furnizarea unor cadre armonizate care să consolideze încrederea și interoperabilitatea în toate statele membre.

Aceste obiective generale răspund provocărilor-cheie identificate în definirea problemei. Acestea reflectă obiectivul general de politică de consolidare a guvernanței în materie de securitate cibernetică în Uniune și de sprijinire a dezvoltării unei piețe unice digitale sigure, reziliente și competitive.

Pentru a contribui la atingerea obiectivelor generale enumerate mai sus, prezenta intervenție urmărește următoarele **obiective specifice (SPO-uri)**:

- pentru a aborda neconcordanța dintre cadrul de politică al Uniunii în materie de securitate cibernetică și nevoile părților interesate:
  - SPO1: crearea capacității de a pune în aplicare în mod eficace politicile Uniunii în materie de securitate cibernetică și cooperarea operațională continuă care să permită o cooperare mai structurată între statele membre;
  - SPO2: dezvoltarea și punerea în aplicare a unor mijloace și mecanisme pentru a sprijini și a aborda în mod eficace nevoile statelor membre, ale industriei și ale altor părți interesate;
- pentru a aborda gradul limitat de adoptare și eficacitatea limitată a ECCF:
  - SPO3: crearea condițiilor prealabile pentru furnizarea mai rapidă a sistemelor de certificare a securității cibernetice determinate de nevoile pieței prin extinderea domeniului de aplicare al ECCF, prin asigurarea unei întrețineri eficace și a unor proceduri flexibile și prin creșterea transparenței;
- pentru a aborda peisajul fragmentat al conformității și complexitatea cadrelor orizontale și sectoriale:
  - SPO4: crearea de mecanisme și condiții pentru a facilita respectarea cerințelor de securitate cibernetică, făcând astfel punerea lor în aplicare mai coerentă și mai eficace.
- pentru a aborda riscurile în materie de securitate cibernetică de la nivelul lanțurilor de aprovizionare:
  - SPO5: Reducerea riscurilor de la nivelul lanțurilor de aprovizionare TIC critice de la entități stabilite în țări terțe sau controlate de entități din țări terțe care prezintă motive de îngrijorare în materie de securitate cibernetică (furnizori cu grad ridicat de risc) și reducerea dependențelor critice prin dezvoltarea unui cadru coerent și eficace la nivelul UE pentru a aborda riscurile la adresa securității lanțurilor de aprovizionare TIC.

Revizuirea Regulamentului privind securitatea cibernetică intră în domeniul de aplicare al **Programului privind o reglementare adecvată și funcțională (REFIT)**. Aceasta contribuie în mod semnificativ la îmbunătățirea clarității, la eliminarea ineficiențelor și la alinierea procedurilor la nivelul cadrelor juridice. Revizuirea Regulamentului privind securitatea

cibernetică contribuie la buna funcționare a pieței interne, asigurând în același timp securitatea și autonomia strategică a Uniunii.

Mai concret, aceasta propune o reformă completă a mandatului Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA), oferind un sprijin eficace pentru punerea în aplicare a politicilor și valoare adăugată în ceea ce privește sprijinirea cooperării operaționale între statele membre.

Având în vedere riscurile și provocările tot mai mari în materie de securitate cibernetică cu care se confruntă Uniunea, propunerea urmărește să sporească resursele financiare și umane ale ENISA pentru a reflecta rolul și sarcinile sale sporite, precum și poziția sa esențială în apărarea ecosistemului digital al Uniunii, permițând ENISA să își îndeplinească în mod eficace sarcinile care îi sunt conferite prin prezenta propunere.

Revizuirea va contribui, de asemenea, la eliminarea practicilor fragmentate, îmbunătățind coordonarea și reducând în același timp costurile de asigurare a conformității și costurile operaționale pe termen lung. Prin abrogarea actualului Regulament privind securitatea cibernetică și prin introducerea unui ECCF reformat, propunerea oferă un instrument mai eficace și mai eficient, care promovează încrederea în rândul întreprinderilor, al publicului larg și al autorităților publice și facilitează respectarea legislației relevante a Uniunii. Aceasta sporește eficiența prin revizuirea modelului de guvernanță și prin sprijinirea unor proceduri de certificare mai previzibile, mai coerente și mai flexibile, pentru a permite dezvoltarea și punerea în aplicare mai rapidă a sistemelor.

O mai mare sinergie cu cadrele juridice relevante existente ale Uniunii va promova certificarea ca instrument de conformitate pentru întreprinderi și va reduce sarcina administrativă a organismelor de evaluare a conformității care își desfășoară activitatea în temeiul mai multor acte legislative în materie de securitate cibernetică. În plus, prin extinderea domeniului de aplicare al ECCF și prin facilitarea dezvoltării unui sistem privind postura de securitate cibernetică a entităților, propunerea reduce costurile de asigurare a conformității pentru entitățile care fac obiectul legislației relevante a Uniunii în materie de securitate cibernetică, începând cu entitățile care intră în domeniul de aplicare al Directivei NIS 2. Această abordare va simplifica în mod semnificativ obligațiile de reglementare pentru entitățile care fac obiectul mai multor cerințe de conformitate și va asigura o utilizare mai eficace a resurselor în rândul autorităților naționale. Pe lângă această revizuire, o propunere de directivă care introduce modificări specifice ale Directivei NIS 2 vizează simplificarea respectării aspectelor specifice ale cadrului de securitate cibernetică și asigurarea unei puneri în aplicare raționalizate și coerente a acestora, inclusiv în ceea ce privește domeniul de aplicare, definițiile, raportarea privind atacurile de tip ransomware și supravegherea entităților care furnizează servicii transfrontaliere.

De asemenea, noul regulament creează un cadru armonizat pentru a aborda riscurile non-tehnice care afectează lanțurile de aprovizionare TIC, reducând fragmentarea actuală a abordărilor între statele membre. Împreună, aceste aspecte reprezintă o simplificare și o modernizare substanțială a cadrului juridic al Uniunii în materie de securitate cibernetică, aliniat pe deplin la principiile REFIT privind claritatea, eficiența și pregătirea digitală.

- **Coerența cu dispozițiile de politică deja existente în domeniul de politică vizat**

Uniunea și-a extins instrumentele juridice și de politică prin adoptarea unei serii de instrumente juridice și de măsuri de politică: (i) Directiva NIS 2 servește la consolidarea securității cibernetice pentru infrastructura critică; (ii) măsurile de securitate fizică sunt definite în „directiva conexă”, Directiva privind reziliența entităților critice; (iii) Regulamentul privind reziliența cibernetică sporește securitatea cibernetică a produselor; (iv) Regulamentul privind solidaritatea cibernetică creează capacități de răspuns la nivelul UE; (v) Planul de acțiune al UE în materie de securitate cibernetică[7] sprijină cooperarea la nivelul UE în materie de gestionare a crizelor, în cadrul căreia Comisia și Înaltul Reprezentant au roluri esențiale în pregătirea pentru incidentele de securitate cibernetică de mare amploare și în răspunsul la acestea; (vi) setul de instrumente pentru securitatea cibernetică a rețelelor 5G (setul de instrumente pentru rețelele 5G) sprijină securitatea cibernetică în rețelele 5G; (vii) planul de acțiune european privind securitatea cibernetică a spitalelor și a furnizorilor de servicii medicale[8] contribuie la îmbunătățirea securității cibernetice a acestora și (viii) Academia de competențe în materie de securitate cibernetică[9] abordează provocarea tot mai mare reprezentată de deficitul de talente în materie de securitate cibernetică.

Cadrul juridic în materie de securitate cibernetică menționat mai sus a fost completat de acte legislative sectoriale, și anume Regulamentul privind reziliența operațională digitală pentru sectorul financiar, codul de rețea privind normele sectoriale pentru aspectele de securitate cibernetică ale fluxurilor transfrontaliere de energie electrică pentru subsectorul energiei electrice sau normele de securitate a informațiilor (Part-IS[10]) pentru subsectorul transportului aerian.

Revizuirea Regulamentului privind securitatea cibernetică este aliniată la dispozițiile NIS 2 privind rolul ENISA în sprijinirea punerii în aplicare a NIS 2 și le consolidează, inclusiv în ceea ce privește sprijinul pentru cooperarea operațională; aceasta este, de asemenea, aliniată la Regulamentul privind reziliența cibernetică, inclusiv în ceea ce privește imaginea de ansamblu și gestionarea vulnerabilităților pe piața internă și sporește valoarea adăugată a conștientizării comune a situației. În ceea ce privește ECCF, revizuirea Regulamentului privind securitatea cibernetică este aliniată la Regulamentul privind reziliența cibernetică în ceea ce privește obiectivele de securitate a produselor și gestionarea vulnerabilităților, precum și la noul cadru legislativ (NCL) privind acreditarea. De asemenea, există o sinergie puternică care decurge din dezvoltarea certificării posturii de securitate cibernetică pentru Directiva NIS 2, precum și, eventual, pentru facilitarea respectării altor acte juridice relevante ale Uniunii, cum ar fi Regulamentul general privind protecția datelor (RGPD), fără a aduce atingere cerințelor lor specifice de certificare. În plus, cadrul orizontal care abordează riscurile în materie de securitate cibernetică de la nivelul lanțurilor de aprovizionare TIC sprijină obiectivul general al Directivei NIS 2 de a crea un nivel comun ridicat de securitate cibernetică în întreaga Uniune și se bazează pe abordarea bazată pe riscuri a Directivei NIS 2.

De asemenea, revizuirea Regulamentului privind securitatea cibernetică, în combinație cu propunerea de directivă de introducere a unor modificări specifice ale Directivei NIS 2 în

---

7 COM(2025) 66 final.

8 COM(2025) 10 final.

9 COM(2023) 207 final.

10 Regulamentul de punere în aplicare (UE) 2023/203 al Comisiei și Regulamentul delegat (UE) 2022/1645 al Comisiei.

scopul simplificării, oferă instrumentele necesare astfel încât acest cadru cuprinzător să devină mai eficace și mai eficient în obținerea rezultatelor preconizate, să ofere o dimensiune europeană mai puternică și să elimine lacunele de reglementare rămase.

- **Coerența cu alte politici ale Uniunii**

Revizuirea Regulamentului privind securitatea cibernetică ar completa Directiva REC, care include considerații privind lanțul de aprovizionare ca parte a măsurilor de reziliență ale entităților critice. În plus, aceasta ar completa inițiativele viitoare, cum ar fi: (i) Regulamentul privind dezvoltarea tehnologiei de tip cloud și a IA (CAIDA), care urmărește, printre altele, să abordeze lipsa unei oferte competitive de servicii de cloud computing la nivelul Uniunii la o scară suficientă pentru a deservi cazuri sau sectoare de utilizare extrem de critice; (ii) propunerea de act legislativ privind rețelele digitale (DNA); (iii) viitoarea revizuire a Regulamentului (UE) 2023/1781[11], (iv) cadrul privind achizițiile publice[12], care este în prezent în curs de evaluare[13], și Propunerea de regulament privind simplificarea legislației digitale (Omnibus digital)[14], care prevede obligația ENISA de a dezvolta un punct unic de intrare pentru raportarea incidentelor, prin care entitățile să își poată îndeplini simultan obligațiile de raportare a incidentelor în temeiul mai multor acte juridice. În plus, aceasta ar consolida poziția autorităților și a operatorilor Uniunii atunci când colaborează cu partenerii din sudul Mediteranei, în special prin promovarea interconectării prin infrastructuri digitale sigure și de încredere în întreaga Mediterană, care este un obiectiv fundamental al Pactului pentru Mediterana.

Revizuirea Regulamentului privind securitatea cibernetică este, de asemenea, în conformitate cu documentele strategice ale Uniunii, în special în ceea ce privește cadrul de securitate a lanțului de aprovizionare TIC. În Strategia ProtectEU, Comisia a afirmat, de asemenea, că o abordare armonizată a securității lanțului de aprovizionare al tehnologiei informației și comunicațiilor (TIC) poate remedia fragmentarea actuală a pieței interne cauzată de abordările diferite la nivel național, poate evita dependențele critice și poate reduce riscul reprezentat de furnizorii cu grad ridicat de risc pentru lanțurile de aprovizionare TIC, securizând astfel infrastructura critică. Strategia pentru securitate economică a subliniat, de asemenea, necesitatea de a spori reziliența economiei și a lanțului de aprovizionare ale UE, în vederea sporirii competitivității Uniunii[15]. Necesitatea de a aborda perturbările lanțurilor de aprovizionare și atacurile cibernetice a fost evidențiată, de asemenea, în Strategia privind o Uniune a pregătirii și în Cartea albă privind apărarea europeană[16]. Aceasta este, de asemenea, aliniată la raportul lui Mario Draghi privind viitorul competitivității europene, astfel cum s-a subliniat mai sus. În plus, revizuirea Regulamentului privind securitatea cibernetică în domeniul securității lanțurilor de aprovizionare TIC prin Comunicarea comună către

---

11 Regulamentul (UE) 2023/1781 al Parlamentului European și al Consiliului din 13 septembrie 2023 de stabilire a unui cadru de măsuri pentru consolidarea ecosistemului european al semiconductorilor și de modificare a Regulamentului (UE) 2021/694 (Regulamentul privind cipurile), *JO L 229, 18.9.2023, p. 1*.

12 În special Directivele 2014/23/UE, 2014/24/UE și 2014/25/UE.

13 Comisia Europeană, Comisia lansează o cerere de contribuții și o consultare publică privind evaluarea directivelor privind achizițiile publice, https://single-market-economy.ec.europa.eu/news/commission-launches-call-evidence-and-public-consultation-evaluation-public-procurement-directives-2024-12-13_en.

14 COM(2025) 837 final.

15 JOIN(2023) 20 final.

16 JOIN(2025) 120 final.

Parlamentul European și Consiliu privind consolidarea securității economice a UE[17], recent adoptată.

2. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

• Temeiul juridic

Temeiul juridic al propunerii îl constituie articolul 114 din Tratatul privind funcționarea Uniunii Europene (TFUE). Articolul 114 din TFUE prevede adoptarea de măsuri pentru a asigura instituirea și funcționarea pieței interne. Regulamentul (UE) 2019/881 privind ENISA și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor, cunoscut sub denumirea de CSA[18], a fost adoptat inițial în temeiul acestei dispoziții.

În domeniul securității cibernetice a securității lanțurilor de aprovizionare TIC, fragmentarea cadrelor naționale care abordează factorii de risc non-tehnic are efecte negative asupra funcționării pieței interne, deoarece divergențele dintre abordările naționale ar putea conduce, în cele din urmă, la o vulnerabilitate mai mare a unor state membre, cu potențiale efecte de propagare în întreaga Uniune, afectând reziliența generală și, de asemenea, credibilitatea.

Având în vedere caracterul evolutiv al amenințărilor la adresa securității cibernetice și interdependența tot mai mare a sistemelor digitale ale statelor membre, articolul 114 din TFUE rămâne temeiul juridic justificat pentru revizuirea Regulamentului privind securitatea cibernetică. Regulamentul propus reflectă cele mai recente evoluții din peisajul legislativ al securității cibernetice, în special având în vedere responsabilitățile tot mai mari ale ENISA și extinderea domeniului de aplicare al certificărilor și al gestionării riscurilor.

• Subsidiaritatea (în cazul competențelor neexclusive)

Principiul subsidiarității impune obligația de a evalua necesitatea și valoarea adăugată a acțiunii Uniunii. Respectarea principiului subsidiarității în acest domeniu a fost deja recunoscută la adoptarea actualului Regulament privind securitatea cibernetică.

Astfel cum s-a analizat deja în legătură cu Regulamentul privind securitatea cibernetică, intervenția Uniunii este esențială, deoarece amenințările la adresa securității cibernetice și provocările conexe se extind dincolo de statele membre individuale. Soluțiile naționale fragmentate s-au dovedit insuficiente pentru a asigura încrederea și coordonarea la nivelul întregii piețe. Este necesar un cadru juridic revizuit al Uniunii pentru a elimina barierele, a asigura punerea în aplicare coerentă și a sprijini statele membre într-un mediu de reglementare și de amenințări din ce în ce mai complex. Securitatea cibernetică este o chestiune de interes comun pentru Uniune.

Acțiunile vizate de propunerea de regulament oferă o valoare adăugată clară prin sprijinirea armonizării, a clarității juridice și a răspunsurilor coordonate la provocările în materie de securitate cibernetică.

Sarcinile actuale ale ENISA s-au extins prin acte legislative ulterioare, fără o revizuire cuprinzătoare a responsabilităților sale de bază și a resurselor de care dispune. Acest lucru a creat ineficiențe și o prioritizare insuficientă a sarcinilor principale în sprijinul statelor membre. Prin urmare, propunerea de intervenție urmărește să perfecționeze și să definească

[17] JOIN(2025) 977 final.

[18] Regulamentul - 2019/881 - RO - EUR-Lex.

nivelul de prioritate al sarcinilor actuale pentru a consolida mandatul ENISA, permițându-i să acționeze ca punct unic de expertiză pentru securitatea cibernetică la nivelul Uniunii. În această privință, nu există nicio diferență substanțială în ceea ce privește subsidiaritatea în comparație cu Regulamentul privind securitatea cibernetică. În plus, diversitatea sistemelor naționale de certificare și abordările diferite în materie de reglementare ale statelor membre creează o fragmentare a pieței și sarcini suplimentare de asigurare a conformității, subminând competitivitatea.

Noua propunere prevede, de asemenea, noi acțiuni în ceea ce privește politicile privind lanțul de aprovizionare și eforturile de simplificare la nivelul Uniunii. Aceasta consolidează și mai mult securitatea lanțului de aprovizionare și sectorul securității cibernetice din Uniune și sporește gradul de pregătire și reziliența statelor membre și a industriei.

Dependențele de entități stabilite într-o țară terță care prezintă motive de îngrijorare privind securitatea cibernetică sau care sunt controlate de o astfel de țară terță, de o entitate stabilită într-o astfel de țară terță sau de un resortisant al unei astfel de țări terțe (furnizori cu grad ridicat de risc) afectează entități din întreaga Uniune, în timp ce incidentele de securitate cibernetică semnificative din lanțul de aprovizionare se răspândesc adesea dincolo de frontierele naționale. În plus, având în vedere caracterul transfrontalier al lanțurilor de aprovizionare TIC, fragmentarea cerințelor de conformitate în cadrul pieței interne ar submina securitatea juridică pentru entități. În plus, propunerile privind cadrul financiar multianual (CFM) prevăd excluderea furnizorilor cu grad ridicat de risc pentru a proteja integritatea bugetului UE și interesele în materie de securitate. Cadrul lanțului de aprovizionare inclus în prezentul regulament prevede mecanismul de identificare a țărilor care prezintă motive de îngrijorare în materie de securitate cibernetică, o activitate care poate fi desfășurată în mod eficace numai la nivelul UE. În ceea ce privește securitatea lanțului de aprovizionare TIC, numai intervenția la nivelul UE va asigura același nivel minim de securitate în întreaga Uniune și armonizarea necesară a abordărilor.

Scopul Regulamentului privind securitatea cibernetică este menținut și consolidat în continuare în cadrul prezentei revizuiri. Acest lucru nu poate fi realizat în mod satisfăcător de către statele membre, dar poate fi realizat mai bine la nivelul Uniunii, în conformitate cu articolul 5 din Tratatul privind Uniunea Europeană.

- **Proporționalitatea**

Măsurile propuse nu depășesc ceea ce este necesar pentru atingerea obiectivelor de politică ale propunerii. În plus, domeniul de aplicare al intervenției Uniunii nu împiedică nicio acțiune națională suplimentară în materie de securitate națională. Prin urmare, acțiunea Uniunii este justificată din rațiuni de subsidiaritate și proporționalitate.

Propunerea urmărește să reflecte mai bine, din punct de vedere juridic, mandatul ENISA și procesul de elaborare, adoptare și menținere a certificatelor europene de securitate cibernetică. Deși propunerea include anumite sarcini noi pentru ENISA, scopul acestora este de a sprijini statele membre în domeniile în care au fost identificate lacune semnificative. ENISA nu va înlocui echipele CSIRT ale statelor membre. În ceea ce privește ECCF, certificarea rămâne voluntară și poate ajuta entitățile să demonstreze conformitatea cu cerințele de securitate cibernetică ale Uniunii. Această abordare asigură respectarea principiului proporționalității.

În ceea ce privește soluțiile propuse în legătură cu securitatea lanțului de aprovizionare TIC, cadrul prevede colectarea de dovezi cu privire la ceea ce constituie active esențiale și la măsurile care ar fi proporționale și necesare pentru a asigura reducerea riscurilor lanțurilor de

aprovizionare critice. Înainte de definirea acestor măsuri, se va efectua o evaluare a impactului economic, care va analiza, printre altele, fezabilitatea economică, alternativele disponibile pe piață, ciclul de viață al produselor specifice. Această evaluare va contribui la măsurile bazate pe riscuri care sunt necesare și cele mai adecvate.

- **Alegerea instrumentului**

Prezenta propunere revizuiește Regulamentul (UE) 2019/881, care stabilește mandatul și sarcinile actuale ale ENISA și ale ECCF. Prin urmare, mandatul revizuit al ENISA și modificările aduse ECCF sunt cel mai bine stabilite în cadrul aceluiași instrument juridic, instrumentul utilizat fiind un regulament. Legislația propusă implică, de asemenea, un cadru eficace la nivelul UE pentru a aborda riscurile în materie de securitate a lanțului de aprovizionare TIC, în cazul căruia un regulament ar aborda mai eficient problemele identificate și ar îndeplini obiectivele formulate, deoarece numai o intervenție la nivelul UE va asigura același nivel de securitate în întreaga Uniune și armonizarea necesară a abordărilor. Procesul de transpunere în cazul unei directive pentru o astfel de intervenție ar putea lăsa prea multă marjă de apreciere la nivel național, ceea ce ar putea duce la lipsa de uniformitate a anumitor cerințe esențiale de securitate cibernetică, la insecuritate juridică, la o fragmentare suplimentară sau chiar la situații transfrontaliere discriminatorii.

3. REZULTATELE EVALUĂRILOR *EX POST*, ALE CONSULTĂRILOR CU PĂRȚILE INTERESATE ȘI ALE EVALUĂRILOR IMPACTULUI

- **Evaluările *ex post*/verificarea adecvării legislației existente**

În conformitate cu articolul 67 din Regulamentul (UE) 2019/881, Comisia Europeană a evaluat relevanța, impactul, eficacitatea, eficiența, coerența și valoarea adăugată a ENISA și a ECCF, având în vedere evoluția peisajului tehnologic și de reglementare. Această evaluare, finalizată în decembrie 2024, a acoperit perioada 2017-2023 și a vizat revizuirea mandatului și a activităților ENISA, precum și evaluarea rolului ECCF în promovarea unui mediu cibernetic securizat în întreaga UE. Principalele constatări pot fi sintetizate după cum urmează:

- **Relevanță:** relevanța ENISA în domeniul securității cibernetice este subliniată de capacitatea sa de reacție la evoluția nevoilor părților interesate și de adaptabilitatea la un peisaj în schimbare. Deși nivelul de satisfacție a părților interesate este, în general, pozitiv, există oportunități de creștere a impactului ENISA. Acest lucru poate fi realizat prin îmbunătățirea sprijinului și a vizibilității pentru diverse sectoare, în special pentru întreprinderile mici și mijlocii (IMM-uri), care se confruntă adesea cu dificultăți în ceea ce privește cerințele în materie de securitate cibernetică. O mai bună organizare a resurselor și o coordonare mai clară cu autoritățile naționale sunt esențiale. Redefinirea priorităților activităților și optimizarea resurselor existente vor alinia mai bine ENISA la nevoile dinamice ale peisajului european al securității cibernetice.

  În ceea ce privește ECCF, în pofida premisei sale promițătoare, se consideră în continuare că acest cadru are un potențial mai mare decât impactul practic, întrucât doar un singur sistem de certificare a devenit recent operațional. Cadrul este conceput pentru a se integra fără probleme cu alte acte juridice ale Uniunii în vederea simplificării procedurilor și a facilitării comerțului transfrontalier. Importanța sa este evidențiată în domenii de înaltă asigurare, cum ar fi serviciile de cloud și infrastructurile 5G.

- **Eficacitatea:** ENISA și-a îndeplinit cu succes mandatul obținând aproape toate realizările planificate, demonstrând flexibilitate și reziliență în timpul unor crize precum pandemia de COVID-19 și războiul de agresiune al Rusiei împotriva Ucrainei. Cu toate acestea, sunt necesare o mai bună definire a priorităților, o orientare clară și o alocare strategică a resurselor pentru a spori eficiența. O abordare mai flexibilă a guvernanței interne este esențială pentru adaptarea la evoluția cerințelor în materie de securitate cibernetică și pentru reducerea la minimum a întârzierilor.

  ECCF a urmărit să armonizeze certificarea securității cibernetice în întreaga Uniune, dar s-a confruntat cu provocări semnificative, inclusiv limitări procedurale și fragmentare, care au condus la întârzieri și ineficiențe, cum ar fi întârzierea adoptării sistemului european de certificare a securității cibernetice bazat pe criterii comune (EUCC). Factorii externi, cum ar fi tensiunile geopolitice și pandemia de COVID-19, au complicat și mai mult realizarea obiectivelor ECCF, subliniind necesitatea unor măsuri adaptabile și a unei alocări coerente a resurselor între părțile interesate pentru a asigura uniformitatea și eficacitatea certificării de securitate cibernetică. În pofida acestor obstacole, au existat rezultate pozitive – în special în ceea ce privește sensibilizarea statelor membre cu privire la importanța și complexitatea certificării de securitate cibernetică.

- **Eficiența:** ENISA a funcționat eficient în cadrul său organizațional bazat pe matrice, promovând cooperarea și definirea priorităților sarcinilor. Cu toate acestea, ENISA s-a confruntat cu provocări în ceea ce privește satisfacerea numărului din ce în ce mai mare al cererilor și ocuparea posturilor specializate, exacerbate de un deficit global de specialiști IT, ceea ce a dus la întârzieri și la un volum mare de muncă. Pentru a aborda aceste probleme, ENISA ar putea să își optimizeze forța de muncă internă și să realoce resursele în mod eficace, astfel cum o demonstrează ajustările strategice, cum ar fi transferul de resurse din 2022 către acțiunea de sprijin în materie de securitate cibernetică. În plus, îmbunătățirea gestiunii bugetare și reducerea cheltuielilor administrative ar îmbunătăți și mai mult eficiența operațională a agenției.

  Eficiența ECCF a fost criticată din cauza termenelor prelungite pentru adoptarea sistemelor de certificare a securității cibernetice și a complexității implicate, primul sistem fiind adoptat abia la începutul anului 2024, la aproape cinci ani de la adoptarea Regulamentului privind securitatea cibernetică. Provocările politice și tehnice, cum ar fi dezbaterile privind suveranitatea datelor și dificultățile legate de transpunerea proiectelor în acte juridice, au contribuit la întârzieri. Provocările politice și cerințele tehnice au împiedicat progresul, astfel cum s-a observat în cazul sistemului UE de certificare în domeniul cloud computingului (EUCS) și al sistemului EU5G. În pofida acestor ineficiențe, cadrul a dat naștere mai multor aspecte pozitive. Cu toate acestea, este în continuare nevoie de îmbunătățiri în ceea ce privește implicarea părților interesate și guvernanța internă pentru a asigura funcționarea optimă și contribuția strategică.

- **Coerența:** coerența ENISA este sprijinită de implicarea semnificativă a părților interesate și de alinierea la cadrele legislative recente. Cu toate acestea, pentru a spori coerența și alocarea resurselor, este esențial să se îmbunătățească sinergiile cu alte organisme ale Uniunii, cum ar fi Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică (ECCC), și cu autoritățile naționale. În plus, trebuie îmbunătățite comunicarea internă și gestionarea resurselor în cadrul ENISA, împreună cu interacțiunea transparentă cu

părțile interesate din sectorul privat. Delimitarea clară a sarcinilor ENISA, în conformitate cu Regulamentul privind reziliența cibernetică și cu Directiva NIS 2, va îmbunătăți atât eficiența, cât și coerența în materie de reglementare.

În ceea ce privește ECCF, coerența deplină cu alte instrumente legislative ale Uniunii, inclusiv cu Directiva NIS 2 și cu Regulamentul privind reziliența cibernetică, este esențială pentru asigurarea unei abordări unificate în materie de securitate cibernetică. Deși ECCF arată o aliniere teoretică la aceste măsuri legislative, în lumea reală integrarea rămâne complexă și necesită o supraveghere atentă. Punerea în aplicare a sistemului EUCC adoptat în cadrul Regulamentului privind reziliența cibernetică va fi un test semnificativ în acest sens.

- **Valoarea adăugată europeană:** ENISA a adus contribuții substanțiale la ecosistemul de securitate cibernetică al Uniunii prin promovarea cooperării și alinierea practicilor. Rolul său în facilitarea eforturilor naționale și în furnizarea de informații cu privire la amenințările emergente a fost vital. Cu toate acestea, criticile formulate de părțile interesate din sectorul privat cu privire la necesitatea unui sprijin mai adaptat indică necesitatea unei mai bune implicări a părților interesate și a unei mai bune colaborări a industriei. Reevaluarea strategică a gestionării resurselor ar permite ENISA să se adapteze mai bine la provocările în continuă evoluție în materie de securitate cibernetică și să deservească mai eficient diverse părți interesate. ECCF a urmărit să introducă procese de certificare armonizate, dar s-a confruntat cu provocări în materie de punere în aplicare din cauza termenelor prelungite și a fragmentării. Valoarea adăugată a ECCF a fost limitată din cauza deficiențelor sale în atingerea obiectivelor și a lipsei sale de eficiență. În pofida acestor provocări, ECCF a îmbunătățit armonizarea între statele membre și a stabilit oportunități de cooperare mai bune, în special prin crearea unor forumuri de cooperare cu părțile interesate, cum ar fi Grupul european pentru certificarea securității cibernetice (ECCG).

- **Consultarea cu părțile interesate**

În perioada 2023-2025, au avut loc mai multe consultări cu părțile interesate, atât în contextul evaluării Regulamentului privind securitatea cibernetică, cât și al revizuirii Regulamentului privind securitatea cibernetică, după cum urmează:

– **în 2023,** au fost realizate 65 de interviuri (dintre care 52 s-au axat mai mult pe ENISA și 13 s-au axat în principal pe ECCF), a fost realizat un program de sondaj, care a primit 209 răspunsuri (dintre care 70 au vizat ECCF), a fost încheiată o consultare publică și au fost organizate două ateliere pe tema analizei SWOT (puncte forte, puncte slabe, șanse și amenințări) și a recomandărilor, cu 26 și, respectiv, 70 de participanți. Aceste activități au vizat în mod specific colectarea opiniilor părților interesate pentru a evalua impactul, eficacitatea și eficiența ENISA. Raportul final al *Studiului de sprijinire a evaluării Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) și a Cadrului european de certificare a securității cibernetice, realizat pentru Comisie de PwC, Intellera Consulting și PPMI (2024)*, a fost finalizat în decembrie 2024*;*

– **în 2025,** Comisia a lansat o cerere de contribuții. În special, părțile interesate au fost invitate să prezinte contribuții scrise, inclusiv documente de poziție, rapoarte tehnice sau observații cu privire la propuneri specifice de reformă. S-au primit în total 184 de contribuții individuale de la o gamă largă de categorii de părți interesate, inclusiv asociații industriale, firme de securitate cibernetică, IMM-uri, instituții academice și organizații de interes public;

– **în perioada aprilie-iunie 2025**, Comisia a organizat o consultare publică ca parte a revizuirii Regulamentului privind securitatea cibernetică și a primit 193 de răspunsuri. Consultarea a constat în 38 de întrebări, atât închise, cât și deschise, care au vizat mandatul ENISA, ECCF, securitatea lanțului de aprovizionare TIC și simplificarea;

– **consultare specifică (interviuri):** au fost realizate o serie de interviuri semistructurate cu anumite părți interesate. Printre acestea s-au numărat reprezentanți ai ENISA, precum și autorități publice naționale care au dezvoltat sau gestionează platforme naționale de raportare. Interviurile s-au axat pe rolul și capacitatea ENISA, pe funcționarea operațională a ECCF, pe provocările practice legate de alinierea proceselor de certificare la nivel național și la nivelul Uniunii, pe sarcinile de raportare și pe obstacolele din calea punerii în aplicare. Aceste discuții au oferit informații calitative care au îmbogățit interpretarea rezultatelor consultării publice și au sprijinit perfecționarea opțiunilor de politică;

– **consultarea reprezentanților statelor membre în cadrul grupului de lucru al Consiliului[19] și în cadrul discuțiilor bilaterale**, în cadrul cărora statele membre și-au putut exprima opiniile cu privire la revizuirea Regulamentului privind securitatea cibernetică;

– **consultare specifică [grupurile din cadrul ECCF – ECCG și Grupul părților interesate pentru certificarea securității cibernetice (SCCG)]:** în calitatea sa de președinte al ambelor grupuri, Comisia a prezentat situația actuală a revizuirii Regulamentului privind securitatea cibernetică în cadrul reuniunilor ECCG din 12 martie și 3 iulie 2025 și în cadrul reuniunii SCCG din 17 martie 2025. În plus, opiniile suplimentare ale experților din partea membrilor ECCG au fost colectate prin intermediul unor chestionare.

Consultarea s-a axat pe cinci domenii principale identificate ca fiind esențiale pentru viitoarea funcționare și coerență a cadrului de securitate cibernetică al Uniunii:

- **mandatul și rolul operațional al ENISA**, inclusiv sprijinul acordat statelor membre și expertiza în domeniul tehnologiilor emergente;
- **eficacitatea cadrului european de certificare a securității cibernetice**, inclusiv a proceselor de guvernanță și dezvoltare;
- **complexitatea și fragmentarea obligațiilor în materie de securitate cibernetică**, acordând atenție sarcinilor de raportare și potențialei simplificări;
- **proporționalitatea cerințelor pentru IMM-uri** și potențialul unor căi diferențiate de asigurare a conformității și
- **impactul societal și economic** al normelor armonizate în materie de securitate cibernetică, inclusiv efectele asupra consumatorilor, drepturilor, inovării și competitivității.
- **Evaluarea impactului**

Revizuirea Regulamentului privind securitatea cibernetică, împreună cu propunerea de directivă de introducere a unor modificări specifice ale Directivei NIS 2, au fost sprijinite de o evaluare a impactului; a se vedea rezumatul de mai jos. Comitetul de control normativ (CCN) a emis un „aviz pozitiv cu rezerve” cu privire la proiectul de raport de evaluare a impactului

[19] Grupul de lucru orizontal pentru chestiuni cibernetice.

retransmis referitor la revizuirea Regulamentului privind securitatea cibernetică[20]. Evaluarea impactului a fost ajustată pentru a răspunde recomandărilor și observațiilor CCN.

Propunerea finală în materie de politică nu se abate de la opțiunile evaluate în cadrul studiului de impact.

Comisia a examinat opțiuni în patru domenii de intervenție, având în vedere obiectivele specifice care trebuie atinse: (1) mandatul ENISA (care face parte, de asemenea, din actualul Regulament privind securitatea cibernetică); (2) ECCF (care face parte, de asemenea, din actualul Regulament privind securitatea cibernetică); (3) modificări specifice ale Directivei NIS 2, cu scopul de a simplifica mandatul ENISA și ECCF, dar care sunt interconectate cu acestea și (4) securitatea lanțului de aprovizionare TIC, care este, de asemenea, relevantă atât pentru ecosistemul NIS 2, cât și pentru ECCF. Fiecare set de opțiuni reprezintă un domeniu de intervenție în sine, fiind în același timp interconectate și relevante unele pentru altele.

Opțiuni de abordare a neconcordanței dintre cadrul de politică al Uniunii în materie de securitate cibernetică și nevoile părților interesate într-un mediu din ce în ce mai ostil

Opțiunea A.1: *Clarificarea mandatului ENISA și stabilirea priorităților* – Această opțiune ar oferi un cadru clar și stabil pentru sarcinile ENISA prin încorporarea sarcinilor stabilite de alte acte legislative.

Opțiunea A.2: *Reformarea mandatului ENISA* – Această opțiune ar abroga și ar înlocui Regulamentul privind securitatea cibernetică, revizuind mandatul agenției.

Opțiunea A.3: *Reformarea mandatului ENISA, cu un accent puternic pe sprijinul operațional* – Această opțiune s-ar baza pe opțiunea A.2. În plus, ENISA ar urma să dezvolte capacități pentru a sprijini în mod direct entitățile prevăzute în Directiva NIS 2 să răspundă la incidentele de securitate cibernetică și să se redreseze în urma acestora, la cererea unui stat membru.

Opțiuni pentru ECCF

Opțiunea B.1: *Clarificarea domeniului de aplicare, a elementelor și a obiectivelor ECCF și introducerea unui mecanism de întreținere* – Această opțiune ar prevedea un nou mecanism de întreținere pentru sisteme, după adoptarea acestora, care să fie pus în aplicare de ENISA.

Opțiunea B.2: *Reformarea ECCF prin revizuirea procedurilor sale și extinderea domeniului de aplicare pentru a facilita simplificarea conformității cu reglementările* – Această opțiune ar abroga Regulamentul privind securitatea cibernetică și l-ar înlocui cu un nou regulament. Pe lângă opțiunea B.1, procedurile legate de solicitarea, dezvoltarea și adoptarea sistemelor ar fi revizuite pentru a îmbunătăți responsabilitatea și eficiența.

Opțiunea B.3: *Reformarea ECCF, astfel cum se prevede în cadrul opțiunii B.2, și introducerea certificării obligatorii pentru postura de securitate cibernetică* – Această opțiune s-ar baza pe opțiunea B.2, dar urmărește să sporească și mai mult impactul cadrului prin introducerea certificării obligatorii a entităților esențiale, luând în considerare scenarii de risc specifice, în loc să se bazeze exclusiv pe certificarea voluntară a entităților.

[20] Regulamentul (UE) 2019/881 (http://data.europa.eu/eli/reg/2019/881/oj).

Opțiuni de simplificare

Opțiunea C.1: *Adoptarea unei abordări bazate pe instrumente juridice neobligatorii și pe instrumente fără caracter legislativ, inclusiv utilizarea delegărilor de competențe existente [adoptarea de acte de punere în aplicare în temeiul articolului 21 alineatul (5) și al articolului 23 alineatul (11) din Directiva NIS 2]* – Această opțiune prevede adoptarea de acte de punere în aplicare utilizând delegările de competențe existente în temeiul Directivei NIS 2 pentru a asigura un grad mai ridicat de armonizare a măsurilor de gestionare a riscurilor în materie de securitate cibernetică, a pragurilor de raportare a incidentelor, precum și a tipului de informații, a formatelor și a procedurii de notificare. Aceasta prevede, de asemenea, adoptarea unui set de orientări pentru a spori securitatea juridică și punerea în aplicare armonizată.

Opțiunea C.2: *Intervenție specifică – simplificarea în continuare a conformității cu cadrul legislativ relevant al Uniunii în materie de securitate cibernetică* – Această opțiune implică o intervenție limitată prin modificări ale Regulamentului privind securitatea cibernetică și ale Directivei NIS 2, cu scopul de a simplifica aspecte specifice ale cadrului de securitate cibernetică, inclusiv adaptările domeniului de aplicare, armonizarea maximă a actelor de punere în aplicare, dovada conformității prin certificare și adoptarea setului de orientări, astfel cum se prevede în opțiunea C.1.

Opțiunea C.3: *Armonizarea măsurilor legate de securitatea cibernetică prevăzute în legislația Uniunii* – Această opțiune s-ar baza pe opțiunea C.2 și ar elimina toate măsurile de gestionare a riscurilor în materie de securitate cibernetică incluse în legislația sectorială și delegările de competențe în legătură cu astfel de măsuri. În schimb, ecosistemul Directivei NIS 2 ar urma să fie modificat pentru a prevedea cerințe raționalizate pentru toate tipurile de entități, cu scopul de a promova armonizarea.

Opțiuni pentru securitatea lanțului de aprovizionare TIC

Opțiunea D.1: Adoptarea unei *abordări bazate pe instrumente juridice neobligatorii pentru a reduce riscurile în materie de securitate cibernetică la nivelul lanțurilor de aprovizionare TIC* – Această opțiune nu ar prevedea o intervenție de reglementare la nivelul UE. În schimb, Comisia ar crește numărul evaluărilor coordonate ale riscurilor și al seturilor de instrumente voluntare.

Opțiunea D.2: *Intervenție de reglementare ad-hoc care codifică setul de instrumente pentru 5G* – Această opțiune ar codifica măsurile din setul de instrumente pentru 5G. Aceasta ar introduce o obligație pentru statele membre de a se asigura că nu sunt utilizate componente de la furnizorii cu grad ridicat de risc în activele esențiale ale rețelei.

Opțiunea D.3: *Un cadru de reglementare cuprinzător și orizontal pentru abordarea riscurilor în materie de securitate cibernetică la nivelul lanțurilor de aprovizionare TIC* – Această opțiune ar institui un cadru de reglementare orizontal, neutru din punct de vedere tehnologic și sectorial pentru a aborda riscurile non-tehnice în materie de securitate cibernetică din lanțurile de aprovizionare TIC.

După o analiză aprofundată, următoarea combinație de opțiuni a devenit pachetul de politici preferat*:* opțiunea A.2 (reformarea mandatului ENISA); opțiunea B.2 (reformarea ECCF prin revizuirea procedurilor sale și extinderea domeniului de aplicare pentru a facilita simplificarea conformității cu reglementările) și opțiunea C.2 (intervenție specifică – simplificarea în continuare a conformității cu cadrul legislativ relevant al Uniunii în materie

de securitate cibernetică) și opțiunea D.3 – Un cadru cuprinzător și orizontal pentru abordarea riscurilor în materie de securitate cibernetică la nivelul lanțurilor de aprovizionare TIC.

Această combinație oferă un răspuns bine echilibrat la provocările identificate în materie de politici, sporind în mod semnificativ eficacitatea, eficiența și coerența în întreaga Uniune.

Tranziția către opțiunea preferată propusă pentru cadrul de reglementare va genera costuri, atât pentru ENISA în vederea îndeplinirii noilor sale sarcini (estimate la până la 161,3 milioane EUR pe o perioadă de cinci ani), cât și pentru autoritățile publice din întreaga Uniune în ceea ce privește supravegherea (estimate la până la 80 de milioane EUR pe o perioadă de cinci ani, având în vedere economiile de costuri relevante). În ceea ce privește întreprinderile, pe o perioadă de cinci ani, eliminarea treptată a anumitor echipamente cu risc ridicat ar putea genera costuri anuale cuprinse între 3,4 și 4,3 miliarde EUR pentru operatorii de rețele de telefonie mobilă, în timp ce investițiile în furnizori de încredere ar putea crește până la 2 miliarde EUR pe an.

În același timp, se preconizează că obligațiile de conformare raționalizate și reduse vor genera economii de costuri de până la 15,3 miliarde EUR pentru întreprinderi pe o perioadă de cinci ani. În plus, îmbunătățirea posturii de securitate cibernetică globale și a suveranității tehnologice a Uniunii și stimularea inovării și a competitivității ar aduce beneficii semnificative publicului larg, autorităților publice și întreprinderilor. Se preconizează că acest lucru va compensa în mare măsură cheltuielile inițiale pe termen lung.

Prin reducerea fragmentării pieței și armonizarea cerințelor de reglementare, opțiunile preferate sporesc egalitatea concurențială în întreaga Uniune, oferind întreprinderilor căi mai clare către conformitate și inovare.

Opțiunile preferate ar contribui, de asemenea, la simplificare prin orientări clare și sisteme integrate, reducând sarcinile administrative. Opțiunile respectă principiul numărului constant, asigurându-se că noile obligații sunt contrabalansate de reduceri în altă parte.

- **Adecvarea reglementărilor și simplificarea**

Revizuirea Regulamentului privind securitatea cibernetică, prin opțiunile de politică A.2, B.2, C.2 și D.3 selectate, contribuie în mod semnificativ la îmbunătățirea clarității, la eliminarea ineficiențelor și la alinierea procedurilor între cadrele juridice. Mai concret, opțiunea A.2 propune o reformă completă a mandatului ENISA, sprijinind în mod eficace punerea în aplicare a politicilor și cooperarea operațională între statele membre. Această consolidare va contribui, de asemenea, la eliminarea practicilor fragmentate, îmbunătățind coordonarea și reducând în același timp costurile de asigurare a conformității și costurile operaționale pe termen lung. Opțiunea B.2, care implică abrogarea actualului Regulament privind securitatea cibernetică și introducerea unui ECCF reformat, sporește eficiența prin revizuirea modelului de guvernanță și prin sprijinirea unor proceduri de certificare mai previzibile, mai coerente și mai flexibile. Acest lucru va permite adoptarea mai rapidă a sistemelor și o mai bună aliniere la legislația transversală, reducând fragmentarea legislativă și reducând sarcina atât pentru părțile interesate publice, cât și pentru cele private. Opțiunea C.2 reduce costurile de asigurare a conformității pentru entitățile care fac obiectul legislației relevante a Uniunii în materie de securitate cibernetică prin modificări ale domeniului de aplicare și permițând instituirea unor sisteme organizaționale de certificare a securității cibernetice pentru entitățile care intră în domeniul de aplicare al Directivei NIS 2 și al altor acte juridice. Această abordare va simplifica în mod semnificativ obligațiile de reglementare pentru entitățile care fac obiectul mai multor cerințe și va asigura o utilizare mai eficace a resurselor în rândul autorităților naționale. Opțiunea D.3 creează un cadru armonizat pentru a aborda riscurile non-tehnice care

afectează lanțurile de aprovizionare TIC, reducând fragmentarea actuală a abordărilor între statele membre. Împreună, aceste opțiuni reprezintă o simplificare și o modernizare substanțială a cadrului juridic al Uniunii în materie de securitate cibernetică, aliniat pe deplin la principiile REFIT privind claritatea, eficiența și pregătirea digitală.

Propunerea este în concordanță cu „verificarea digitală”, deoarece accentul pus de aceasta pe procesele digitale raționalizate demonstrează angajamentul Uniunii față de o abordare de tipul „digitalizarea pe primul loc”, asigurând un schimb de date și un proces decizional mai rapide și mai fiabile. Opțiunea D.3 ar putea avea, de asemenea, un impact ridicat asupra digitalizării, deoarece ar implica înlocuirea componentelor de la entități stabilite în țări terțe sau controlate de entități din țări terțe care prezintă motive de îngrijorare în materie de securitate cibernetică (furnizori cu grad ridicat de risc).

- **Drepturile fundamentale**

Propunerea legislativă a fost evaluată din punct de vedere al potențialului său de a consolida sau de a pune în pericol drepturile fundamentale și de a promova egalitatea și încrederea, cu un accent deosebit pe impactul la nivelul societății și pe drepturi, inclusiv viața privată, protecția datelor și capacitatea persoanelor de a-și înțelege și exercita drepturile și de a asigura respectarea acestora.

Extinderea mandatului ENISA va contribui la o mai mare reziliență cibernetică în întreaga economie și societate în general, conducând la o mai bună protecție a vieții private și a datelor cu caracter personal ale persoanelor. Propunerea va sprijini, de asemenea, educația și formarea în domeniul securității cibernetice, deoarece clarifică rolul ENISA în dezvoltarea competențelor forței de muncă din domeniul securității cibernetice.

În plus, ECCF va spori încrederea publicului larg și a întreprinderilor din Uniune în soluțiile TIC certificate care sprijină viața de zi cu zi. Instituirea unor sisteme suplimentare ar spori acest impact.

Propunerea contribuie la încrederea cetățenilor prin stimularea entităților din sectoarele critice să obțină certificarea securității cibernetice, demonstrând astfel public nivelul lor ridicat de securitate cibernetică. În plus, prin asigurarea unei raportări armonizate cu privire la incidentele care implică atacuri de tip ransomware și prin luarea de măsuri pentru tranziția către criptografia post-cuantică, aceasta ar spori încrederea publicului în protecția datelor sensibile în sectoarele critice.

Dispozițiile privind securitatea lanțului de aprovizionare vor avea un anumit impact asupra protecției drepturilor fundamentale prin limitarea ingerințelor străine. Activități precum spionajul și supravegherea subminează grav drepturile fundamentale ale cetățenilor. Acest cadru orizontal ar avea potențialul de a îmbunătăți încrederea, securitatea și confidențialitatea în diferite tehnologii și soluții digitale.

4. IMPLICAȚII BUGETARE

Bugetul estimat al Agenției UE pentru Securitate Cibernetică (ENISA), care va contribui la o creștere semnificativă a securității UE, a fost estimat la 341 de milioane EUR pentru 7 ani sau la un buget mediu anual de 49 de milioane EUR (proiecție pentru perioada 2028-2034). Aceasta reprezintă o creștere de 81,5 % față de bugetul agenției în 2025. Beneficiile generate de inițiativa propusă, astfel cum sunt analizate în evaluarea impactului, vor fi semnificative, cu economii de costuri de până la 14,6 miliarde EUR pentru întreprinderi. În plus, deși amploarea economiilor potențiale de costuri legate de îmbunătățirea generală a pregătirii

Uniunii împotriva incidentelor de securitate cibernetică este, prin natura sa, dificil de cuantificat, se estimează că economiile de costuri legate de un răspuns mai rapid și de încetinirea proliferării incidentelor de securitate cibernetică ar putea varia între 3,7 și 4,4 miliarde EUR pe o perioadă de cinci ani. În contextul viitoarelor inițiative de politică, Comisia va analiza distribuția generală a resurselor pentru instituțiile, organele, agențiile și oficiile europene în domeniul securității cibernetice și în cadrul acestora, pentru a valorifica cunoștințele și expertiza și pentru a identifica și a dezvolta sinergii.
Resursele suplimentare propuse pentru consolidarea agenției sunt transpuse în 118 ENI și costuri operaționale suplimentare care vor acoperi actualele acorduri de contribuție dintre ENISA și Comisie, cum ar fi întreținerea Platformei unice de raportare; pentru ENI care lucrează la funcționarea și administrarea rezervei UE pentru securitate cibernetică, precum și pentru inițiative importante ale Comisiei, cum ar fi dezvoltarea punctului unic de intrare în temeiul propunerii Omnibus digital. Alte costuri operaționale sunt legate de programul de divulgare coordonată a vulnerabilităților, de colectarea și analiza informațiilor privind amenințările la adresa securității cibernetice, de comunicațiile securizate și de consolidarea maturității în materie de securitate cibernetică pentru ENISA. Costurile operaționale pentru întreținerea sistemelor europene de certificare a securității cibernetice, a autorizațiilor de competențe în materie de securitate cibernetică și a serviciului de instrumente de testare sunt, de asemenea, adăugate în acest buget, însă aceste costuri includ și mecanisme de autofinanțare prin taxe.

Un aspect important al propunerii este introducerea unor mecanisme de taxare care, printre alte obiective de politică, vor contribui, de asemenea, la un circuit financiar sustenabil în cadrul agenției. Regulamentul revizuit privind securitatea cibernetică prezintă trei tipuri de taxe care vor contribui la bugetul ENISA, și anume taxele pentru eliberarea autorizațiilor de atestare a competențelor, taxele pentru serviciul de instrumente de testare și taxele pentru sprijinirea întreținerii sistemelor europene de certificare a securității cibernetice. Beneficiile generate preconizate pentru bugetul UE sunt estimate la aproximativ 18,5 milioane EUR pe o perioadă de 7 ani, din 2028 până în 2034.

Solicitarea bugetară a Comisiei se traduce în 50 de posturi ENI suplimentare, care vor pune în aplicare cadrul privind lanțul de aprovizionare, precum și sarcini legate de elaborarea de acte de punere în aplicare pentru mecanismele de taxare, întreținerea sistemelor de certificare, standardizare și sprijin pentru cooperarea operațională, printre altele. Potrivit estimărilor, costurile suportate de Comisie pentru punerea în aplicare a cadrului privind lanțul de aprovizionare vor fi afectate în mod specific de numărul de evaluări pe care le va efectua Comisia referitoare la structura de proprietate și la mecanismele de control. Cu toate acestea, rezultatele acestei sarcini vor contribui în mare măsură la realizarea de economii pentru statele membre atunci când supraveghează punerea în aplicare a măsurilor de atenuare și a obligațiilor impuse entităților NIS 2 prin acest cadru. Statele membre vor fi în măsură să valorifice rezultatele evaluărilor referitoare la structura de proprietate și la mecanismele de control în mod direct, față de situația în care fiecare în parte ar cheltui resurse pentru aceleași nevoi de evaluare.

Pentru informații mai detaliate, a se vedea fișa financiară care însoțește pachetul cibernetic.

5. ALTE ELEMENTE

- **Planurile de punere în aplicare și măsurile de monitorizare, evaluare și raportare**

Comisia va monitoriza aplicarea regulamentului propus și va prezenta Parlamentului European și Consiliului, o dată la cinci ani, un raport privind evaluarea sa. Aceste rapoarte vor fi publice și vor prezenta în detaliu punerea în aplicare efectivă și asigurarea respectării regulamentului propus.

- **Documentele explicative (în cazul directivelor)**

Nu se aplică, deoarece propunerea este un regulament.

- **Explicarea detaliată a dispozițiilor specifice ale propunerii**

Propunerea clarifică rolul ENISA și îi încredințează sarcini concrete de sprijinire a părților sale interesate, în fruntea cărora se află statele membre, în special în ceea ce privește sprijinul pentru punerea în aplicare a politicii și a legislației Uniunii, cooperarea operațională, consolidarea capacităților, certificarea și standardizarea în materie de securitate cibernetică și îmbunătățirea forței de muncă din domeniul securității cibernetice și a mobilității acesteia în întreaga Uniune. Propunerea urmărește, de asemenea, creșterea eficienței și a eficacității Cadrului european de certificare a securității cibernetice (ECCF) pentru a îmbunătăți nivelul de securitate cibernetică în Uniune și pentru a le permite clienților să facă alegeri în cunoștință de cauză atunci când achiziționează produse, servicii, procese și servicii de securitate gestionate în cadrul pieței interne. În plus, în combinație cu propunerea de directivă de introducere a unor modificări specifice ale Directivei NIS 2, prezenta propunere urmărește să faciliteze respectarea obligațiilor în materie de securitate cibernetică și să deblocheze resurse pentru a consolida pregătirea operațională în materie de securitate cibernetică a entităților din sectoarele critice ale Uniunii. În cele din urmă, propunerea abordează necesitatea de a spori reziliența economiei Uniunii și a lanțului de aprovizionare TIC pentru a-și promova propria securitate și competitivitate. Detaliile sunt furnizate mai jos.

TITLUL I: DISPOZIȚII GENERALE

Titlul I din propunerea de regulament cuprinde dispozițiile generale: obiectul (articolul 1) și definițiile (articolul 2), inclusiv trimiterile la definițiile relevante din alte instrumente ale Uniunii, cum ar fi Directiva (UE) 2022/2555[21] (Directiva NIS 2), Regulamentul (CE) nr. 765/2008[22] și Regulamentul (UE) nr. 1025/2012[23].

TITLUL II: ENISA (AGENȚIA UNIUNII EUROPENE PENTRU SECURITATE CIBERNETICĂ)

Titlul II din propunerea de regulament conține dispozițiile-cheie referitoare la ENISA.

Capitolul I prezintă misiunea (articolul 3) și obiectivele ENISA (articolul 4).

Capitolul II prezintă sarcinile agenției în trei secțiuni.

21 http://data.europa.eu/eli/dir/2022/2555/oj
22 http://data.europa.eu/eli/reg/2008/765/oj
23 http://data.europa.eu/eli/reg/2012/1025/oj

Secțiunea 1 include dispoziții privind sarcinile legate de sprijinirea punerii în aplicare a politicii și a dreptului Uniunii. Aceasta specifică entitățile și organizațiile care urmează să primească sprijin și modul în care ar trebui să se facă acest lucru (articolul 5). Articolul 6 delimitează responsabilitățile agenției în materie de consolidare a capacităților, inclusiv oferirea de cunoștințe și expertiză statelor membre cu privire la prevenirea și soluționarea amenințărilor cibernetice, actualizarea strategiilor de securitate cibernetică și extinderea forței de muncă din domeniul securității cibernetice. ENISA va sprijini, de asemenea, statele membre în activitățile lor de sensibilizare (articolul 7), va efectua analize ale principalelor tendințe ale pieței în materie de securitate cibernetică și va disemina consiliere tehnică și analize (articolul 8). ENISA va contribui, de asemenea, la cooperarea internațională în materie de securitate cibernetică, astfel cum este descrisă la articolul 9, și o va promova.

Secțiunea 2 stabilește sarcinile ENISA în ceea ce privește cooperarea operațională în legătură cu statele membre, entitățile Uniunii și CERT-UE, rețeaua echipelor de intervenție în caz de incidente de securitate informatică (CSIRT), EU-CyCLONe și alte părți interesate, inclusiv emiterea de orientări și punerea în aplicare a unor instrumente de comunicații securizate (articolul 10). ENISA va contribui, de asemenea, la îmbunătățirea conștientizării situației amenințărilor și incidentelor cibernetice prin (printre altele) crearea unuia sau mai multor registre de informații privind amenințările cibernetice, prin efectuarea de analize și emiterea de alerte timpurii (articolul 11). Normele privind astfel de alerte timpurii (conținut, calendar, serviciu) sunt prevăzute la articolul 12. Pentru a ajuta entitățile esențiale și importante să se pregătească pentru incidentele de tip ransomware, să răspundă la acestea și să se redreseze în urma lor, ENISA operează rezerva UE pentru securitate cibernetică, astfel cum se explică la articolul 13 și în cooperare cu Europol și CSIRT sau cu alte autorități competente, după caz. Articolul 14 include dispoziții privind rolul ENISA în exercițiile de securitate cibernetică la nivelul Uniunii, inclusiv compilarea unui program anual continuu de exerciții de securitate cibernetică la nivelul Uniunii. Pe lângă aceste sarcini, ENISA ar trebui să furnizeze instrumente și platforme, în special platforma unică de raportare instituită în temeiul articolului 16 alineatul (1) din Regulamentul (UE) 2024/2847 (articolul 15). În cele din urmă, agenția trebuie să dezvolte o capacitate comună a Uniunii de servicii de gestionare a vulnerabilităților și să furnizeze servicii de gestionare a vulnerabilităților (articolul 16).

Secțiunea 3 privind certificarea și standardizarea securității cibernetice stabilește sarcinile agenției în această privință. Articolul 17 descrie rolul ENISA în dezvoltarea și punerea în aplicare a ECCF, inclusiv rolul său de lider în pregătirea sistemelor și în asigurarea întreținerii și consolidării capacităților acestora, în timp ce articolul 18 stabilește modul în care ENISA ar trebui să se implice în elaborarea specificațiilor tehnice și să contribuie la activitățile de standardizare la nivel european și internațional, inclusiv în domeniul algoritmilor criptografici.

Secțiunea 4 detaliază sarcinile agenției în ceea ce privește punerea în aplicare a Academiei de competențe în materie de securitate cibernetică. Articolul 19 include dispoziții referitoare la rolul ENISA în ceea ce privește cadrul european de competențe în materie de securitate cibernetică (ECSF), în timp ce sarcinile sale privind dezvoltarea și întreținerea sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică sunt prevăzute la articolul 20. Cerințele pentru a deveni furnizor de atestate autorizat sunt prevăzute la articolul 21, iar cele referitoare la prelucrarea cererilor la articolul 22. ENISA trebuie să furnizeze informații publice referitoare la ECSF și la atestările individuale de competențe în materie de securitate cibernetică (articolul 23).

Capitolul III se referă la organizarea ENISA. Structura administrativă și de conducere a agenției include și un director executiv adjunct (articolul 24). Dispozițiile referitoare la consiliul de administrație, componența, președintele, reuniunile, funcțiile și regulile de vot ale acestuia sunt incluse în secțiunea 1 (articolele 25-29). Comitetul executiv trebuie să asiste consiliul de administrație, astfel cum se prevede la articolul 30 din secțiunea 2. Secțiunea 3 include norme privind numirea, revocarea și prelungirea mandatului directorului executiv (articolul 31) și norme privind sarcinile și responsabilitățile directorului executiv (articolul 32). Consiliul de administrație poate decide să creeze un post de director executiv adjunct care să îl asiste pe directorul executiv (secțiunea 4, articolele 33 și 34). Consiliul de administrație trebuie să instituie Grupul consultativ al ENISA, care trebuie să ofere consultanță ENISA în conformitate cu normele prevăzute la articolul 35. Secțiunea 6 stabilește norme privind crearea și componența comisiei pentru soluționarea contestațiilor (articolul 36) și a membrilor acesteia (articolul 37). Articolul 38 precizează circumstanțele în care membrii comisiei pentru soluționarea contestațiilor trebuie să se abțină de la inițierea unei proceduri de contestație și prezintă motivele pentru care se pot formula obiecții cu privire la orice membru al comisiei. Deciziile luate de ENISA pot fi contestate în fața comisiei pentru soluționarea contestațiilor sau în cazul în care ENISA nu acționează (articolul 39). Articolul 40 include dispoziții privind persoanele care au dreptul la o cale de atac, termenul și forma căii de atac. Articolele 41-43 stabilesc norme privind revizuirea preliminară, examinarea deciziilor privind recursurile și acțiunile în fața Curții de Justiție. În final, articolul 44 prevede procesul legat de documentul unic de programare.

Capitolul IV se referă la întocmirea și structura bugetului agenției, precum și la normele care reglementează prezentarea și execuția acestuia (articolele 45-55). Acesta include, de asemenea, dispoziții care facilitează combaterea fraudei, a corupției și a altor activități ilegale (articolul 51).

Capitolul V se referă la dotarea cu personal a agenției. Acesta cuprinde dispoziții generale privind Statutul funcționarilor și Regimul aplicabil celorlalți agenți, precum și normele care reglementează privilegiile și imunitățile (articolele 56 și 57). Acesta introduce dispoziții care impun statelor membre să desemneze ofițeri de legătură în calitate de experți naționali detașați la ENISA și rolul acestora în cadrul agenției (articolul 58). Acesta include, de asemenea, dispoziții care orientează utilizarea experților naționali detașați și a altor categorii de personal care nu sunt angajate de agenție (articolul 59).

În sfârșit, capitolul VI cuprinde dispozițiile generale referitoare la agenție. Acesta prezintă statutul juridic al agenției (articolul 60), stabilește sediul acesteia (articolul 61) și conține dispoziții privind acordul privind sediul și condițiile de funcționare ale agenției, precum și privind controlul administrativ exercitat de Ombudsman (articolele 62 și 63). Acesta include dispoziții care reglementează aspectele legate de răspundere, regimul lingvistic și protecția datelor cu caracter personal (articolele 64-66), precum și norme de securitate privind protecția informațiilor sensibile neclasificate și clasificate (articolul 67). Acesta prevede norme pentru cooperarea cu entitățile Uniunii și cu autoritățile naționale (articolul 68) și cu alte părți interesate (articolul 69). Acesta descrie normele care reglementează cooperarea agenției cu țări terțe și cu organizații internaționale (articolul 70).

TITLUL III: CADRUL EUROPEAN DE CERTIFICARE A SECURITĂȚII CIBERNETICE

Titlul III din propunerea de regulament instituie ECCF.

Capitolul I prezintă obiectivele, domeniul de aplicare și procedurile cadrului. Obiectivele (articolul 71) includ consolidarea securității cibernetice în întreaga Uniune și facilitarea unei abordări armonizate a certificării produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate sau a posturii de securitate cibernetică a entităților. Cadrul ar trebui, de asemenea, să stimuleze certificarea pentru a simplifica conformitatea cu legislația aplicabilă a Uniunii prin prezumția de conformitate, reducând astfel sarcina pentru întreprinderi (articolul 78). Capitolul I detaliază apoi aspectele procedurale, începând cu consultările privind prioritățile strategice europene în materie de certificare a securității cibernetice și informațiile publice legate de dezvoltarea sistemelor de către Comisie și de crearea unei noi Adunări europene pentru certificarea securității cibernetice (articolul 72). În urma unei solicitări detaliate din partea Comisiei (articolul 73), se preconizează că ENISA va prezenta o propunere de sistem în termen de 12 luni. Articolul 74 prevede termene suplimentare legate de prezentarea avizului ECCG și de prezentarea sistemului în vederea adoptării sale de către Comisie. Articolul 75 introduce un mecanism clar de întreținere pentru sistemele existente, care ar putea conduce la revizuirea unor astfel de sisteme (articolul 76). Revizuirea unui sistem s-ar putea baza în continuare pe o evaluare periodică a eficacității și a impactului sistemului asupra pieței unice. Articolul 77 oferă ENISA o bază pentru elaborarea de specificații tehnice în sprijinul dezvoltării și întreținerii sistemelor europene de certificare a securității cibernetice. Atunci când adoptă sau revizuiește un sistem, Comisia poate include trimiteri la aceste specificații tehnice (articolul 74). Diferitele proceduri asigură transparența și calitatea furnizării prin implicarea experților și a părților interesate generale în diferite etape ale planificării, dezvoltării, adoptării și întreținerii sistemelor de certificare. Articolul 79 prevede un site al ENISA dedicat sistemelor europene de certificare a securității cibernetice, care ar trebui să furnizeze informații cu privire la sistemele adoptate, precum și cu privire la certificatele europene de securitate cibernetică și la declarațiile de conformitate UE emise în cadrul sistemelor respective.

Capitolul II prevede norme generale pentru conținutul sistemelor europene de certificare a securității cibernetice.

Articolul 80 stabilește o listă de obiective de securitate în raport cu care ENISA trebuie să conceapă un sistem și asigură alinierea la legislația relevantă în materie de securitate cibernetică. Fiecare sistem european de certificare a securității cibernetice poate prevedea elementele specificate la articolul 81. Aceste elemente trebuie să fie compatibile cu legislația Uniunii și pot fi armonizate între sisteme utilizând dispoziții standard. Ambele dispoziții oferă flexibilitatea necesară pentru a se adapta la diferite tipuri de sisteme. Dispoziții suplimentare specifică normele referitoare la nivelurile de asigurare (articolul 82) și la autoevaluarea conformității (articolul 83). Capitolul stabilește, de asemenea, o listă de informații suplimentare (articolul 84) pe care producătorul sau furnizorul de produse TIC, de servicii TIC sau de procese TIC trebuie să le pună la dispoziție.

În cele din urmă, capitolul III stabilește normele de guvernanță pentru ECCF, împărțite în trei secțiuni.

Secțiunea 1 se referă la normele privind eliberarea certificatelor europene de securitate cibernetică, inclusiv a celor de la nivelul de asigurare „ridicat” (articolul 85). În plus, aceasta stabilește norme pentru armonizarea sistemelor europene de certificare a securității cibernetice cu sistemele naționale de certificare a securității cibernetice și cu certificatele de securitate cibernetică (articolul 86) și prevede posibilitatea recunoașterii internaționale a certificatelor europene de securitate cibernetică, pe baza principiului echivalenței (articolul 87). Secțiunea prezintă, de asemenea, rolul autorităților naționale de certificare a

securității cibernetice și normele aplicabile acestora (articolul 88) și stabilește norme pentru un mecanism de evaluare *inter pares* între aceste autorități, asigurând standarde echivalente în întreaga Uniune (articolul 89), precum și pentru cooperarea dintre aceste autorități în cadrul ECCG (articolul 90).

Secțiunea 2 prevede: (i) norme armonizate privind acreditarea și autorizarea organismelor de evaluare a conformității (articolele 91-92); (ii) norme privind notificarea, inclusiv o împuternicire pentru a asigura alinierea în continuare la dreptul relevant al Uniunii și la NCL (articolul 93) și (iii) o procedură de contestare (articolul 94) care să asigure respectarea cerințelor pentru organismele de evaluare a conformității.

În cele din urmă, secțiunea 3 prevede drepturi și căi de atac împotriva deciziilor legate de certificare (articolul 96) și impune statelor membre să stabilească și să aplice sancțiuni proporționale pentru încălcările reglementărilor.

TITLUL IV

Capitolul I articolul 98 stabilește domeniul de aplicare al cadrului privind lanțul de aprovizionare TIC de încredere. Cadrul va aborda riscurile non-tehnice din sectoarele cu o importanță critică ridicată și din alte sectoare critice, astfel cum sunt menționate în Directiva (UE) 2022/2555. Mecanismul identifică activele TIC esențiale din lanțurile de aprovizionare TIC critice și stabilește măsuri de atenuare adecvate și proporționale cu privire la tipurile de entități menționate în anexele I și II la Directiva (UE) 2022/2555. Cadrul se va baza pe evaluări coordonate la nivelul Uniunii ale riscurilor de securitate, solicitate de Comisie sau de cel puțin trei state membre. Articolul 99 detaliază modul în care vor fi efectuate aceste evaluări ale riscurilor și faptul că acestea ar trebui, de asemenea, să stabilească măsuri de atenuare. Aceste evaluări ale riscurilor ar trebui finalizate în termen de șase luni de la solicitare. La cererea Comisiei, Grupul de cooperare NIS poate conveni asupra unei perioade mai scurte. Cadrul prevede posibilitatea unei proceduri de urgență în cazul în care o intervenție imediată este justificată pentru a menține buna funcționare a pieței interne și în cazul în care Comisia are motive suficiente să considere că există o amenințare cibernetică semnificativă pentru securitatea Uniunii în ceea ce privește lanțurile de aprovizionare TIC critice. În acest caz, Comisia consultă statele membre cu privire la necesitatea de a lua una sau mai multe măsuri de atenuare și efectuează o evaluare a riscurilor. Articolul 100 prevede că, în cazul în care, ca urmare a evaluării riscurilor menționate la articolul 99 sau pe baza altor surse, cum ar fi o declarație publică în numele Uniunii sau al unui stat membru, reiese că o țară terță prezintă riscuri non-tehnice grave și structurale pentru lanțurile de aprovizionare TIC, Comisia verifică amenințarea reprezentată de țara respectivă, ținând seama de elementele enumerate la articolul 100. În cazul în care Comisia concluzionează că o țară terță prezintă riscuri non-tehnice grave și structurale pentru lanțurile de aprovizionare TIC, articolul 100 prevede o procedură prin care Comisia desemnează o astfel de țară terță ca țară care prezintă motive de îngrijorare legate de securitatea cibernetică a lanțurilor de aprovizionare TIC. Entităților stabilite într-o țară terță care prezintă motive de îngrijorare în materie de securitate cibernetică desemnate în conformitate cu acest articol sau controlate de o astfel de țară terță, de o entitate stabilită într-o astfel de țară terță sau de un resortisant al unei astfel de țări terțe nu li se va permite să desfășoare o serie de activități specificate la acest articol. Articolul 101 prevede un mecanism general al lanțului de aprovizionare TIC în cadrul căruia, după finalizarea evaluării riscurilor în materie de securitate de către Grupul de cooperare NIS sau de către Comisie în conformitate cu articolul 99, Comisia poate lua măsurile prevăzute la articolele 102 și 103.

Comisia poate identifica, prin acte de punere în aplicare, activele TIC esențiale utilizate pentru fabricarea de produse și furnizarea de servicii de către tipurile de entități menționate în anexele I și II la Directiva (UE) 2022/2555. Articolul 102 detaliază în continuare elementele care trebuie luate în considerare pentru identificarea activelor TIC esențiale. Articolul 103 stabilește potențialele măsuri de atenuare în cadrul lanțului de aprovizionare TIC. Comisia, prin intermediul unor acte de punere în aplicare, poate decide că entitățile care își desfășoară activitatea în sectoare cu o importanță critică ridicată și în alte sectoare critice trebuie să facă obiectul unor măsuri de atenuare specifice, detaliate în continuare în articol.

Comisia stabilește, prin intermediul unor acte de punere în aplicare, liste cu furnizorii cu grad ridicat de risc relevanți pentru interdicțiile prevăzute în actele de punere în aplicare adoptate în conformitate cu articolul 103 alineatele (1) și (7) sau cu interdicția menționată la articolul 110 alineatul (1), după efectuarea unei evaluări privind stabilirea, proprietatea și controlul. Aceasta ar trebui să consulte furnizorii în cauză și autoritățile competente (articolul 104).

O entitate stabilită într-o țară terță sau controlată de entități dintr-o țară terță care prezintă motive de îngrijorare în materie de securitate cibernetică desemnate în conformitate cu articolul 100 poate solicita să i se permită să furnizeze componente TIC în activele TIC esențiale ale entităților de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555 și să participe la achiziții publice în legătură cu furnizarea unor astfel de componente TIC. Articolul 105 precizează ce ar trebui să conțină cererea și care este procedura pentru o astfel de derogare. Articolul 106 precizează dreptul la apărare al unei entități în cauză. Comisia ține un registru accesibil publicului al deciziilor privind derogările (articolul 107). Articolele 108 și 109 precizează normele de confidențialitate și taxele legate de procedura de derogare.

Capitolul II prevede o aplicare a cadrului privind lanțul de aprovizionare TIC de încredere la rețelele de comunicații electronice mobile, fixe și prin satelit, asigurând alinierea la propunerea de act legislativ privind rețelele digitale.

Activele TIC esențiale pentru rețelele de comunicații electronice mobile, fixe și prin satelit sunt prevăzute în anexa II. Perioada de tranziție pentru eliminarea treptată a componentelor TIC de la furnizorii cu grad ridicat de risc pentru activele TIC esențiale ale rețelei de comunicații electronice mobile nu trebuie să depășească 36 de luni de la intrarea în vigoare a prezentului regulament. Perioadele de tranziție pentru rețelele de comunicații electronice fixe și prin satelit sunt specificate de Comisie în temeiul unor acte de punere în aplicare. Comisia este împuternicită să adopte un act delegat pentru a modifica activele TIC esențiale desemnate și perioadele de tranziție, inclusiv pentru generațiile mobile viitoare (articolul 110). Articolul 111 prevede că furnizorii de rețele de comunicații electronice mobile, fixe și prin satelit nu pot utiliza, instala sau integra, sub nicio formă, componente TIC de la furnizori cu grad ridicat de risc și nu li se poate acorda o autorizație generală sau individuală.

Autoritățile competente, supravegherea și asigurarea respectării legii, jurisdicția, dreptul la apărare (capitolul III)

Capitolul III stabilește, de asemenea, normele privind autoritățile competente, supravegherea, asigurarea respectării legii și jurisdicția.

Articolele 112-114 precizează competențele, mijloacele și responsabilitățile statelor membre în ceea ce privește asigurarea punerii în aplicare și a respectării dispozițiilor din titlul IV. Statele membre trebuie să desemneze una sau mai multe autorități competente, care să fie notificate Comisiei. Articolul 113 prevede instituirea de către Comisie a unei rețele de cooperare între autoritățile competente ale statelor membre și Comisie pentru a facilita

conformitatea, în timp ce articolul 114 precizează măsurile de supraveghere și de asigurare a respectării legislației pe care autoritățile competente au dreptul să le ia. Sancțiunile în cazul încălcării dispozițiilor titlului IV sunt specificate la articolul 115. Articolul 116 detaliază posibilitatea ca statele membre să își acorde reciproc asistență atunci când entitățile desfășoară activități transfrontaliere sau atunci când activele TIC esențiale ale acestora sunt situate în mai multe state membre. Articolul 117 prevede normele privind competența și teritorialitatea.

TITLUL VI: DISPOZIȚII FINALE

Titlul VI din propunerea de regulament include dispozițiile finale, definind normele de adoptare a actelor de punere în aplicare și a actelor delegate, procesul de evaluare a propunerii de regulament, precum și abrogarea și succesiunea Regulamentului (UE) 2019/881. Acesta precizează, de asemenea, data intrării în vigoare a regulamentului propus.

2026/0011 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), cadrul european de certificare a securității cibernetice și securitatea lanțului de aprovizionare TIC și de abrogare a Regulamentului (UE) 2019/881 (Regulamentul privind securitatea cibernetică 2)

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 114,

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European[24],

având în vedere avizul Comitetului Regiunilor[25],

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) De la adoptarea Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului[26], peisajele geopolitice, tehnologice și de politică au suferit transformări semnificative. Indiferent dacă sunt cauzate de defecțiuni ale sistemului, de erori umane, de acte răuvoitoare sau de fenomene naturale, incidentele de securitate cibernetică s-au înmulțit, iar atacurile cibernetice au devenit mai sofisticate, afectând entitățile esențiale, întreprinderile și publicul larg. Ecosistemul criminalității informatice s-a dezvoltat, în centrul său aflându-se activitatea de tip ransomware. S-au intensificat incidentele la nivelul lanțurilor de aprovizionare, indiferent dacă sunt cauzate de infractori pentru câștiguri financiare sau de actori statali pentru perturbare, spionaj, dezinformare sau război. Ca parte a unei strategii hibride mai ample, incidentele care rezultă din activități cibernetice răuvoitoare și din disfuncționalități ale sistemelor se propagă în exterior, perturbând serviciile esențiale, subminând încrederea în instituții și afectând pregătirea Uniunii la nivelul societății și pregătirea pentru apărare a Uniunii. Astfel de incidente și-au dovedit potențialul de a afecta activitatea economică, stabilitatea financiară și viața oamenilor. În același timp,

[24] JO C , , p. .

[25] JO C , , p. .

[26] Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

vulnerabilitatea infrastructurii și a sistemelor civile critice prezintă un risc pentru capabilitățile de apărare atunci când acestea se bazează pe ele.

(2) În paralel, tehnologiile emergente, cum ar fi inteligența artificială și informatica cuantică, au un efect perturbator asupra securității cibernetice și a apărării cibernetice. Acestea remodelează instrumentele de apărare și tacticile adversarilor, reprezentând amenințări la adresa securității cibernetice și a apărării cibernetice și oferind, în același timp, căi pentru progrese tehnologice. Deși pot contribui la securitatea cibernetică prin îmbunătățirea detectării amenințărilor sau a răspunsului automatizat la incidente, acestea măresc, de asemenea, suprafața generală de atac pentru organizații, sunt ținte potențiale ale manipulării și pot submina viabilitatea pe termen lung a măsurilor de securitate, cum ar fi criptarea.

(3) Pentru a aborda aceste evoluții, Uniunea și-a consolidat instrumentele juridice și de politică. Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[27] consolidează securitatea cibernetică pentru infrastructura critică, completată de Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului[28] în ceea ce privește securitatea fizică. Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului[29] consolidează securitatea cibernetică a produselor cu elemente digitale. Regulamentul (UE) 2025/38 al Parlamentului European și al Consiliului[30] consolidează capacitățile de răspuns la nivelul Uniunii, iar Recomandarea Consiliului din 6 iunie 2025 privind un Plan de acțiune al UE pentru gestionarea crizelor cibernetice[31] („Recomandarea privind Planul de acțiune în materie de securitate cibernetică”) sprijină cooperarea în materie de gestionare a crizelor la nivelul Uniunii. Setul de instrumente pentru securitatea cibernetică a rețelelor 5G[32] constituie un prim pas către o abordare coordonată la nivelul Uniunii pentru securizarea rețelelor 5G. Comunicarea Comisiei privind Academia de competențe în materie de securitate cibernetică[33] abordează provocarea tot mai mare reprezentată de deficitul de talente în

---

27 Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (JO L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

28 Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului (JO L 333, 27.12.2022, p. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).

29 Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentelor (UE) nr. 168/2013 și (UE) 2019/1020, precum și a Directivei (UE) 2020/1828 (Regulamentul privind reziliența cibernetică) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

30 Regulamentul (UE) 2025/38 al Parlamentului European și al Consiliului din 19 decembrie 2024 de stabilire a unor măsuri de consolidare a solidarității și a capacităților la nivelul Uniunii pentru detectarea amenințărilor și a incidentelor de securitate cibernetică, pregătirea legată de acestea și răspunsul la acestea și de modificare a Regulamentului (UE) 2021/694 (Regulamentul privind solidaritatea cibernetică) (JO L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

31 JO C, C/2025/3445, 20.6.2025, ELI: http://data.europa.eu/eli/C/2025/3445/oj.

32 Securitatea cibernetică a rețelelor 5G – Setul de instrumente al UE privind măsurile de atenuare a riscurilor, Grupul de cooperare NIS, 1/2020, disponibil la adresa: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

33 Comunicarea Comisiei către Parlamentul European și Consiliu, Eliminarea deficitului de talente în materie de securitate cibernetică pentru a stimula competitivitatea, creșterea și reziliența UE („Academia de competențe în materie de securitate cibernetică”), COM(2023) 207 final, 18 aprilie 2023.

materie de securitate cibernetică. În plus, cadrul de securitate cibernetică a fost consolidat de legislația sectorială, în special de Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului[34] pentru sectorul financiar, de Regulamentul delegat (UE) 2024/1366 al Comisiei[35] pentru subsectorul energiei electrice, de Regulamentul delegat (UE) 2022/1645 al Comisiei[36] și de Regulamentul de punere în aplicare (UE) 2023/203 al Comisiei[37](PART-IS), precum și de normele relevante în materie de securitate a aviației prevăzute în Regulamentul (UE) 2019/1583 al Comisiei[38] pentru subsectorul transportului aerian și de alte documente de politică, cum ar fi Comunicarea Comisiei referitoare la un plan de acțiune al UE privind securitatea cibernetică a spitalelor și a furnizorilor de servicii medicale[39]. Entitățile Uniunii sunt, de asemenea, consolidate prin Regulamentul (UE, Euratom) 2023/2841 al Parlamentului European și al Consiliului[40], care stabilește măsuri ce vizează atingerea unui nivel comun ridicat de securitate cibernetică în cadrul instituțiilor, organelor, oficiilor și agențiilor Uniunii. Acest cadru juridic consolidat pentru securitatea cibernetică a specificat mai în detaliu sarcinile ENISA.

---

34 Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

35 Regulamentul delegat (UE) 2024/1366 al Comisiei din 11 martie 2024 de completare a Regulamentului (UE) 2019/943 al Parlamentului European și al Consiliului prin stabilirea unui cod de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică (JO L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

36 Regulamentul delegat (UE) 2022/1645 al Comisiei din 14 iulie 2022 de stabilire a normelor de aplicare a Regulamentului (UE) 2018/1139 al Parlamentului European și al Consiliului în ceea ce privește cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației impuse organizațiilor care intră sub incidența Regulamentelor (UE) nr. 748/2012 și (UE) nr. 139/2014 ale Comisiei și de modificare a Regulamentelor (UE) nr. 748/2012 și (UE) nr. 139/2014 ale Comisiei (JO L 248, p. 18, 26.9.2022, ELI: http://data.europa.eu/eli/reg_del/2022/1645/oj).

37 Regulamentul de punere în aplicare (UE) 2023/203 al Comisiei din 27 octombrie 2022 de stabilire a normelor de aplicare a Regulamentului (UE) 2018/1139 al Parlamentului European și al Consiliului în ceea ce privește cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, impuse organizațiilor care intră sub incidența Regulamentelor (UE) nr. 1321/2014, (UE) nr. 965/2012, (UE) nr. 1178/2011, (UE) 2015/340 ale Comisiei și a Regulamentelor de punere în aplicare (UE) 2017/373 și (UE) 2021/664 ale Comisiei, precum și autorităților competente care intră sub incidența Regulamentelor (UE) nr. 748/2012, (UE) nr. 1321/2014, (UE) nr. 965/2012, (UE) nr. 1178/2011, (UE) 2015/340 și (UE) nr. 139/2014 ale Comisiei și a Regulamentelor de punere în aplicare (UE) 2017/373 și (UE) 2021/664 ale Comisiei, și de modificare a Regulamentelor (UE) nr. 1178/2011, (UE) nr. 748/2012, (UE) nr. 965/2012, (UE) nr. 139/2014, (UE) nr. 1321/2014, (UE) 2015/340 ale Comisiei și a Regulamentelor de punere în aplicare (UE) 2017/373 și (UE) 2021/664 ale Comisiei (JO L 31, 2.2.2023, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2023/203/oj).

38 Regulamentul de punere în aplicare (UE) 2019/1583 al Comisiei din 25 septembrie 2019 de modificare a Regulamentului de punere în aplicare (UE) 2015/1998 de stabilire a măsurilor detaliate de implementare a standardelor de bază comune din domeniul securității aviației în ceea ce privește măsurile de securitate cibernetică (JO L 246, 26.9.2019, p. 15, ELI: http://data.europa.eu/eli/reg_impl/2019/1583/oj).

39 Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor, Plan de acțiune european privind securitatea cibernetică a spitalelor și a furnizorilor de servicii medicale, COM(2025) 10 final, 15 ianuarie 2025.

40 Regulamentul (UE, Euratom) 2023/2841 al Parlamentului European și al Consiliului din 13 decembrie 2023 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii (JO L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

(4) În acest context și astfel cum se menționează în ProtectEU: Strategia europeană de securitate internă[41] și Strategia privind o Uniune a pregătirii[42] arată că pregătirea, securitatea și reziliența societății și economiei Uniunii necesită, de pe o parte, o coordonare europeană solidă, încredere și schimb de informații între părțile interesate, cadre solide care să garanteze securitatea produselor, serviciilor, proceselor TIC și a serviciilor de securitate gestionate, și, de pe altă parte, creșterea și consolidarea forței de muncă din domeniul securității cibernetice. De asemenea, este necesară consolidarea lanțurilor de aprovizionare TIC prin asigurarea suveranității tehnologice europene asupra activelor esențiale, ceea ce ar spori reziliența Uniunii și ar putea aduce beneficii eforturilor de apărare cibernetică. În plus, Comunicarea privind consolidarea securității economice a UE[43] identifică drept obiective prioritare necesitatea de a preveni accesul la informații și date sensibile care ar putea submina securitatea economică a UE și de a preveni și a atenua perturbările infrastructurii critice a UE care afectează economia UE. Aceasta recunoaște rolul esențial pe care îl joacă măsurile eficace de securitate cibernetică în această privință.

(5) Incidentele de securitate cibernetică de mare amploare care afectează infrastructura critică, serviciile digitale sau funcțiile societale esențiale pot avea un impact asupra populației, necesitând acțiuni coordonate de protecție civilă și de gestionare a crizelor la nivelul Uniunii. În conformitate cu abordarea care ține seama de toate pericolele din Strategia europeană privind o Uniune a pregătirii și cu Decizia 1313/2013/UE privind mecanismul de protecție civilă al Uniunii, mecanismele de conștientizare a situației, de răspuns la incidente și de exerciții în temeiul prezentului regulament ar trebui să contribuie la gestionarea crizelor la nivelul Uniunii, în special prin intermediul Centrului de coordonare a răspunsului la situații de urgență (ERCC).

(6) Prezenta propunere este în concordanță cu (Propunerea de directivă de completare a [revizuirii Regulamentului (UE) 2019/881] și de modificare a Directivei (UE) 2022/2555 în ceea ce privește simplificarea punerii în aplicare a măsurilor pentru un nivel comun ridicat de securitate cibernetică în Uniune), precum și cu [Propunerea de regulament privind simplificarea legislației digitale (Omnibus digital)][44], care prevede obligația ENISA de a dezvolta un punct unic de intrare pentru raportarea incidentelor prin care entitățile să își poată îndeplini simultan obligațiile de raportare a incidentelor în temeiul mai multor acte juridice și este completată de acestea.

(7) Regulamentul (CE) nr. 460/2004 al Parlamentului European și al Consiliului[45] a instituit ENISA cu scopul de a contribui la obiectivele de asigurare a unui nivel ridicat și eficace al securității rețelelor și a informațiilor în Uniune și la dezvoltarea unei culturi a securității rețelelor și a informațiilor, în beneficiul cetățenilor, al consumatorilor, al întreprinderilor și al administrațiilor publice. Mandatul ENISA a

---

41 Comunicarea Comisiei Către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor privind ProtectEU: o strategie europeană de securitate internă, COM(2025) 148 final, 1 aprilie 2025.

42 Comunicare comună a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor referitoare la Strategia europeană privind o Uniune a pregătirii, JOIN(2025) 130 final.

43 Comunicare comună a Comisiei către Parlamentul European și Consiliu, Consolidarea securității economice a UE, JOIN(2025) 977 final.

44 COM(2025) 837 final.

45 Regulamentul (CE) nr. 460/2004 al Parlamentului European și al Consiliului din 10 martie 2004 privind instituirea Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor (JO L 77, 13.3.2004, p. 1, ELI: http://data.europa.eu/eli/reg/2004/460/oj).

fost prelungit de trei ori înainte să i se acorde un mandat permanent prin Regulamentul (UE) 2019/881. Pentru a răspunde mai bine nevoilor create de evoluția amenințărilor și a peisajelor tehnologice, în special în ceea ce privește cooperarea operațională și nevoia tot mai mare de profesioniști în domeniul securității cibernetice, mandatul ENISA ar trebui consolidat în continuare. Din motive de securitate juridică, Regulamentul (UE) 2019/881 ar trebui înlocuit.

(8) Într-un peisaj al amenințărilor în continuă evoluție, în care incidentele de securitate cibernetică devin din ce în ce mai semnificative, asigurarea încrederii persoanelor fizice, a autorităților publice și a întreprinderilor în utilizarea zilnică a tehnologiilor este chiar mai importantă ca niciodată. O creștere a încrederii poate fi facilitată printr-o certificare consolidată la nivelul Uniunii a ECCF care să prevadă cerințe comune în materie de securitate cibernetică și criterii de evaluare aplicabile pe toate pieţele naționale și în toate sectoarele. Noul cadru ar trebui să stabilească principalele cerințe orizontale pentru sistemele europene de certificare a securității cibernetice și să permită recunoașterea și utilizarea certificatelor europene de securitate cibernetică și a declarațiilor de conformitate UE în toate statele membre. În acest sens, Comisia ar trebui să stabilească o procedură și un cadru de guvernanță care să permită dezvoltarea și întreținerea în timp util și în mod previzibil a sistemelor europene de certificare a securității cibernetice. Sistemele europene de certificare a securității cibernetice ar trebui să se aplice în mod uniform în toate statele membre pentru a asigura o punere în aplicare armonizată a cerințelor de securitate cibernetică, pentru a asigura condiții de concurență echitabile și pentru a preveni practica de căutare a certificării celei mai avantajoase, în funcție de nivelurile diferite de strictețe din diferite state membre. ENISA ar trebui să aibă un rol esențial în asigurarea dezvoltării sistemelor prin specificații tehnice și în asigurarea faptului că aceste sisteme rămân actualizate din punct de vedere tehnic. În plus, pentru a răspunde în mod eficace nevoilor pieței, cadrul ar trebui să prevadă posibilitatea certificării măsurilor de gestionare a riscurilor în materie de securitate cibernetică adresate entităților și să faciliteze respectarea altor acte legislative aplicabile ale Uniunii în domeniul securității cibernetice. Alinierea la legislația existentă a Uniunii, cum ar fi Regulamentul (UE) 2024/2847 și Directiva (UE) 2022/2555, este esențială pentru ca sistemele europene de certificare a securității cibernetice să contribuie la reducerea sarcinii de asigurare a conformității pentru întreprinderi, să le sporească atractivitatea și să consolideze reziliența cibernetică a Uniunii.

(9) Misiunea ENISA ar trebui să fie de a sprijini statele membre și entitățile Uniunii să atingă un nivel ridicat de securitate cibernetică, reziliență și încredere în Uniune. În acest scop, ENISA ar trebui să acționeze ca punct de referință pentru consiliere și expertiză în materie de securitate cibernetică, iar activitatea sa ar trebui să se axeze în principal pe patru domenii-cheie ale securității cibernetice la nivelul Uniunii. În primul rând, ENISA ar trebui să sprijine statele membre în punerea în aplicare coerentă a politicii și a legislației Uniunii în materie de securitate cibernetică și să asiste statele membre prin activități de consolidare a capacităților pentru a-și îmbunătăți în permanență capacitățile în ceea ce privește pregătirea, reziliența și răspunsul. În al doilea rând, ENISA ar trebui să contribuie la cooperarea operațională la nivelul Uniunii, între statele membre, și la o mai bună conștientizare comună a situației în ceea ce privește amenințările și incidentele cibernetice între statele membre și entitățile Uniunii. Al treilea domeniu-cheie ar trebui să fie certificarea și standardizarea securității cibernetice, în timp ce al patrulea ar trebui să fie punerea în aplicare a Academiei de competențe în materie de securitate cibernetică, care ar trebui să contribuie la dezvoltarea unei forțe de muncă europene prospere în domeniul

securității cibernetice, cu competențe care ar trebui să fie portabile în toate statele membre.

(10) Regulamentul (UE, Euratom) 2023/2841 de stabilire a unor măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii prevede mandatul CERT-UE, instituindu-l ca serviciu de securitate cibernetică pentru instituțiile, organele, oficiile și agențiile Uniunii, pentru a contribui la securitatea mediului TIC neclasificat al entităților Uniunii prin consilierea acestora cu privire la securitatea cibernetică, ajutându-le să prevină, să detecteze, să gestioneze, să atenueze, să răspundă la incidente și să se redreseze în urma acestora și acționând ca centru de schimb de informații în materie de securitate cibernetică și de coordonare a răspunsului la incidente. În plus, CERT-UE are sarcina de a oferi servicii de securitate cibernetică relevante entităților Uniunii. Ca parte a misiunii sale, ENISA ar trebui să sprijine și entitățile Uniunii. În special, ar trebui să facă acest lucru prin implicarea printr-o cooperare structurată cu CERT-UE în ceea ce privește consolidarea capacităților, cooperarea operațională și analizele strategice pe termen lung ale amenințărilor cibernetice. După caz, ENISA poate valorifica cooperarea structurată cu CERT-UE pentru serviciile de securitate cibernetică ale ENISA sau sprijinul care poate aduce valoare adăugată entităților Uniunii, în mod coordonat, pentru a asigura sinergii cu eforturile CERT-UE.

(11) Una dintre sarcinile principale ale ENISA ar trebui să fie sprijinirea statelor membre în punerea în aplicare consecventă a politicii și legislației Uniunii în materie de securitate cibernetică, în special în ceea ce privește Directiva (UE) 2022/2555, Regulamentul (UE) 2024/2847 și Regulamentul (UE) 2025/38. Pentru a contribui la punerea în aplicare coerentă și eficace a acquis-ului Uniunii în materie de securitate cibernetică, ENISA ar trebui să emită orientări și rapoarte tehnice, să ofere consiliere și bune practici și să faciliteze schimbul de bune practici între autoritățile competente în acest scop. În plus, ENISA evaluează situația în materie de securitate cibernetică în Uniune și adoptă un raport în acest sens în conformitate cu articolul 18 din Directiva (UE) 2022/2555. ENISA ar trebui, de asemenea, să fie în măsură să răspundă cererilor de consiliere și asistență din partea statelor membre și, după caz, a entităților Uniunii, cu privire la aspecte care intră sub incidența mandatului ENISA.

(12) În vederea stimulării cooperării dintre sectorul public și cel privat și în cadrul sectorului privat, în special pentru a sprijini protecția infrastructurii critice, ENISA ar trebui să sprijine schimbul de informații în cadrul sectoarelor și între acestea, în special în sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555, precum și de informații privind produsele cu elemente digitale care intră în domeniul de aplicare al Regulamentului (UE) 2024/2847. Acest sprijin poate lua forma furnizării de bune practici și orientări cu privire la instrumentele și procedurile disponibile, precum și a furnizării de orientări cu privire la modul de abordare a aspectelor de reglementare legate de schimbul de informații, de exemplu prin facilitarea înființării de centre sectoriale de schimb de informații și de analiză (ISAC).

(13) Pentru a sprijini și a facilita cooperarea strategică și schimbul de informații, ENISA ar trebui să contribuie la activitatea grupului de cooperare instituit prin Directiva (UE) 2022/2555 („Grupul de cooperare NIS”), în special prin furnizarea de expertiză și consiliere și prin facilitarea schimbului de bune practici, printre altele, în ceea ce privește dependențele transfrontaliere legate de riscuri și incidente. ENISA ar trebui, de asemenea, să contribuie la activitatea Grupului european de cooperare privind

identitatea digitală instituit prin Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului[46], a Grupului european pentru certificarea securității cibernetice și a Grupului de cooperare administrativă (ADCO) instituit prin Regulamentul (UE) 2024/2847.

(14) Nucleul public al internetului deschis, și anume principalele sale protocoale și infrastructura, care constituie un bun public global, oferă funcționalitatea esențială a internetului în ansamblu și susține funcționarea sa normală. În cadrul mandatului său, ENISA ar trebui să sprijine securitatea și reziliența nucleului public al internetului deschis și stabilitatea funcționării acestuia, inclusiv, dar fără a se limita la acestea, implementarea și operarea în condiții de siguranță a protocoalelor-cheie (în special sistemul de nume de domenii, protocolul Border Gateway și versiunea 6 a protocolului de internet) și operarea sistemului de nume de domenii (cum ar fi operarea tuturor domeniilor de prim nivel), prin promovarea celor mai bune practici, a orientărilor și a cooperării, în conformitate cu acordurile globale și multipartite stabilite privind guvernanța internetului și cu rolurile și responsabilitățile respective ale organismelor tehnice și operaționale internaționale relevante.

(15) ENISA acționează ca punct de referință pentru consiliere și expertiză în materie de securitate cibernetică. Prin urmare, la cererea Comisiei, ENISA ar trebui să îi acorde asistență prin expertiză, consiliere tehnică, informații, analize, inclusiv studii de fezabilitate, avize și activități pregătitoare cu privire la orice aspect specific din domeniul securității cibernetice, cu scopul de a contribui la elaborarea politicilor Comisiei și de a facilita monitorizarea de către Comisie a punerii în aplicare a legislației Uniunii în materie de securitate cibernetică.

(16) În mod similar, ținând seama de expertiza sa, ENISA ar trebui să furnizeze asistență statelor membre în eforturile lor de a crea și de a consolida capacitățile și pregătirea necesare pentru a preveni, a detecta și a răspunde la amenințările cibernetice și incidentele și în ceea ce privește securitatea rețelelor și a sistemelor informatice. În special, ENISA ar trebui să sprijine dezvoltarea și consolidarea echipelor de intervenție în caz de incidente de securitate informatică („echipe CSIRT”) prevăzute în Directiva (UE) 2022/2555, astfel încât să se ajungă la un nivel comun ridicat de maturitate a echipelor CSIRT în Uniune.

(17) ENISA a sprijinit și ar trebui să sprijine în continuare statele membre în elaborarea și punerea în aplicare a orientărilor pentru strategiile lor naționale de securitate cibernetică, contribuind la adoptarea și punerea în aplicare a strategiilor de securitate cibernetică de către toate statele membre. ENISA ar trebui să promoveze diseminarea acestor strategii prin intermediul hărții interactive a strategiilor naționale de securitate cibernetică (NCSS) și ar trebui să urmărească în continuare progresele înregistrate în punerea lor în aplicare, inclusiv prin acordarea de sprijin în elaborarea indicatorilor-cheie de performanță în acest context.

(18) Regulamentul (UE, Euratom) 2023/2841 a însărcinat Consiliul interinstituțional pentru securitate cibernetică să sprijine entitățile Uniunii în ridicarea posturilor lor respective de securitate cibernetică, iar CERT-UE să contribuie la securitatea mediului TIC neclasificat al tuturor entităților Uniunii. Pe baza experienței sale în materie de

[46] Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE (JO L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

securitate cibernetică, ENISA ar trebui să sprijine Consiliul interinstituțional pentru securitate cibernetică și CERT-UE în sarcinile lor în conformitate cu Regulamentul (UE, Euratom) 2023/2841, inclusiv prin contribuția la analiza amenințărilor cibernetice, conștientizarea situației, exercițiile de securitate cibernetică, coordonarea răspunsului la incidente și schimbul de know-how și de bune practici.

(19) Pe baza expertizei ENISA și pentru a completa capacitățile autorităților publice naționale și ale Uniunii, ENISA ar trebui să ofere cursuri de formare utilizând ca bază Cadrul european de competențe în materie de securitate cibernetică (ECSF), în special pentru a sprijini punerea în aplicare eficace a politicilor, cooperarea operațională și sensibilizarea.

(20) Pentru a asigura sinergii cu Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică (ECCC) și cu Rețeaua de centre naționale de coordonare instituită în temeiul Regulamentului (UE) 2021/887 al Parlamentului European și al Consiliului[47], ENISA ar trebui să le sprijine prin schimbul de informații cu privire la riscurile și amenințările cibernetice actuale și emergente, inclusiv la riscurile și amenințările legate de tehnologiile informației și comunicațiilor.

(21) Strategia de pregătire subliniază că alfabetizarea digitală, care se bazează pe dobândirea de competențe digitale de bază, este esențială pentru a capacita cetățenii astfel încât să fie mai reziliențI în fața potențialelor crize. Cu toate acestea, astfel cum s-a subliniat în Comunicarea Comisiei privind uniunea competențelor[48], aproape jumătate din populația adultă nu are competențe digitale de bază, în pofida faptului că peste 90 % din locurile de muncă necesită astfel de competențe. Pentru a se asigura că forța de muncă actuală și cea potențială viitoare au competențele necesare într-un mediu digital care evoluează rapid și pentru a contribui la dezvoltarea rezervei europene de talente în materie de securitate cibernetică, ENISA ar trebui să sprijine activitățile de sensibilizare în materie de securitate cibernetică care vizează atragerea de talente și să contribuie la informarea cu privire la educația și competențele necesare în domeniul securității cibernetice, cum ar fi provocarea europeană în materie de securitate cibernetică. În acest sens, ENISA ar trebui să coordoneze concursuri în materie de securitate cibernetică, evenimente de inventariere și exerciții practice similare, ca mijloc de dezvoltare a competențelor în materie de securitate cibernetică și de promovare a consolidării capacităților în întreaga Uniune. Atunci când desfășoară activități de sensibilizare, ENISA ar trebui să se asigure că acestea răspund nevoilor autorităților publice naționale și ale entităților Uniunii, precum și nevoilor întreprinderilor, în special ale IMM-urilor, și ale instituțiilor de educație și formare, prin menținerea unor cadre practice și a unor cursuri de formare, cum ar fi sensibilizarea într-un cadru unic. ENISA ar trebui să elaboreze în continuare orientări practice și realizabile pentru a sprijini punerea în aplicare a politicii și a legislației Uniunii în materie de securitate cibernetică. Totodată, ENISA ar trebui să depună

---

47 Regulamentul (UE) 2021/887 al Parlamentului European și al Consiliului din 20 mai 2021 de înființare a Centrului european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică și a Rețelei de centre naționale de coordonare (JO L 202, 8.6.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

48 Comunicare a Comisiei către Parlamentul European, Consiliul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor, Uniunea competențelor, COM(2025) 90 final, 5 martie 2025.

eforturi pentru a oferi informații relevante despre sistemele de certificare aplicabile, furnizând, de exemplu, orientări și recomandări.

(22) Pentru a sprijini întreprinderile care își desfășoară activitatea în sectorul securității cibernetice și utilizatorii de soluții de securitate cibernetică și pentru a asigura punerea în aplicare eficace a titlului III din prezentul regulament, ENISA ar trebui să dezvolte și să mențină un „observator al pieței” prin efectuarea de analize periodice și diseminarea de informații cu privire la principalele tendințe de pe piața securității cibernetice, în ceea ce privește atât cererea, cât și oferta. În plus, pentru a sprijini utilizatorii rezervei UE pentru securitate cibernetică instituite în temeiul Regulamentului (UE) 2025/38, ENISA ar trebui să pregătească cartografierea serviciilor de care au nevoie acești utilizatori și a disponibilității unor astfel de servicii, în temeiul regulamentului respectiv.

(23) Amenințările pentru securitatea cibernetică au o dimensiune mondială. Este necesară o cooperare internațională mai strânsă pentru a îmbunătăți securitatea cibernetică, inclusiv pentru a defini norme comune de comportament și abordări comune. În acest scop, ENISA ar trebui să sprijine cooperarea Uniunii cu țările terțe, cu accent pe țările candidate la aderarea la Uniune, și cu organizațiile internaționale, cum ar fi NATO, furnizând expertiza și analizele necesare Comisiei și entităților relevante ale Uniunii, după caz. Activitățile ENISA în domeniul internațional ar trebui să fie întotdeauna în conformitate cu prioritățile Uniunii.

(24) Pentru a contribui la atingerea unui nivel ridicat de securitate cibernetică în Uniune, ENISA ar trebui să sprijine cooperarea operațională între statele membre, în cooperare cu CERT-UE, între entitățile Uniunii și între părțile interesate. În acest scop, rolul ENISA ar trebui consolidat. ENISA ar trebui să devină membru al rețelei CSIRT, contribuind la schimbul de informații și la analiza din cadrul rețelei. ENISA ar trebui să promoveze și să sprijine în continuare cooperarea dintre echipele CSIRT relevante în caz de incidente, atacuri sau perturbări ale rețelelor sau ale infrastructurii gestionate sau protejate de echipele CSIRT. Sprijinul activ al ENISA pentru activitatea rețelei CSIRT și a Rețelei europene a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe) ar trebui să permită acestor rețele să își consolideze în continuare nivelul de maturitate. Rolul ENISA în sprijinirea unei astfel de cooperări include combaterea amenințărilor la adresa securității și integrității instituțiilor democratice, a alegerilor și a altor procese, precum și a infrastructurii critice de care depind acestea, în conformitate cu Scutul european pentru democrație: consolidarea democrațiilor puternice și reziliente[49].

(25) Pentru a sprijini consolidarea capacităților, cooperarea operațională și analizele strategice pe termen lung ale amenințărilor cibernetice, ENISA ar trebui să utilizeze expertiza tehnică și operațională disponibilă a CERT-UE printr-o cooperare structurată, de exemplu prin acorduri specifice.

(26) Pentru a consolida securitatea cibernetică în întreaga Uniune și pentru a asigura un răspuns rapid și eficace la amenințările cibernetice, ENISA ar trebui să sprijine statele membre, la cererea acestora, inclusiv prin furnizarea de consiliere cu privire la îmbunătățirea capacităților lor de prevenire, detectare a incidentelor, răspuns la acestea și redresare în urma acestora, prin facilitarea gestionării tehnice a incidentelor semnificative în sensul Directivei (UE) 2022/2555, în special prin sprijinirea schimbului voluntar de soluții tehnice între statele membre sau prin asigurarea faptului

[49] JOIN(2025) 791 final.

că sunt analizate amenințările cibernetice și incidentele. De asemenea, ENISA ar trebui să sprijine EU-CyCLONe în elaborarea rapoartelor către nivelul politic al Uniunii și al statelor membre.

(27) Pentru a reduce expunerea la ingerințe străine, la manipularea lanțului de aprovizionare și la exfiltrarea strategică a datelor, ENISA ar trebui să utilizeze instrumente de comunicații securizate în cadrul rețelei CSIRT și al EU-CyCLONe. Pe baza Recomandării privind Planul de acțiune în materie de securitate cibernetică, astfel de instrumente ar trebui să fie furnizate de entități juridice stabilite sau considerate a fi stabilite în Uniune și controlate de statele membre sau de resortisanți ai statelor membre.

(28) Pentru a contribui la pregătirea și răspunsul la nivelul Uniunii în cazul unor incidente și crize de securitate cibernetică de mare amploare, ENISA ar trebui să desfășoare activități de conștientizare a situației în materie de securitate cibernetică.

(29) Accesul la informații privind amenințările cibernetice în timp real, verificate și fiabile este esențial pentru conștientizarea comună a situației în Uniune. ENISA, Comisia, CERT-UE și Centrul european de combatere a criminalității informatice (EC3) din cadrul Europol au dezvoltat deja registre de informații privind amenințările cibernetice care sunt adaptate la nevoile lor specifice. ENISA și alte entități relevante ale Uniunii ar trebui să coopereze în mod voluntar pentru a crea registre de informații privind amenințările cibernetice în timp real, verificate și fiabile și să caute sinergii pentru a asigura economii de scară și pentru a consolida buna gestiune financiară. Această activitate ar trebui să includă și entități sectoriale ale Uniunii, cum ar fi Agenția UE pentru Programul spațial. Acestea ar trebui să partajeze numai analize, tendințe și tactici, tehnici și proceduri derivate, nu și surse brute, și ar trebui să respecte independența entităților de a-și gestiona propriul ciclu de viață al informațiilor privind amenințările cibernetice în conformitate cu mandatele lor și cu normele privind necesitatea de a cunoaște.

(30) Pentru a contribui la un răspuns prompt și coordonat, ENISA ar trebui să poată emite alerte timpurii cu privire la un incident semnificativ sau de mare amploare potențial sau în curs sau la o amenințare cibernetică de natură transfrontalieră potențială către echipa CSIRT sau echipele CSIRT în cauză și, după caz, către rețeaua de echipe CSIRT și EU-CyCLONe, în special în ceea ce privește entitățile enumerate în anexele I și II la Directiva (UE) 2022/2555. Informațiile din astfel de alerte timpurii pot include vulnerabilități cunoscute public și dacă acestea afectează produse cu elemente digitale care intră sub incidența Regulamentului (UE) 2024/2847, precum și tehnici și proceduri, indicatori de compromis, tactici contradictorii, informații specifice despre actorii care generează amenințări și recomandări privind măsurile de atenuare.

(31) Pentru a menține încrederea și a nu pune în pericol schimbul de informații, este important ca ENISA să aplice marcaje vizibile care să indice măsura în care un document sau o informație pe care a produs-o sau a primit-o poate face obiectul unui schimb ulterior. În mod similar, ENISA ar trebui să utilizeze documentele sau informațiile pe care le primește în scopul desfășurării activităților sale, sub rezerva oricăror limitări prin intermediul unui marcaj vizibil privind distribuirea ulterioară a informațiilor respective.

(32) Pentru a contribui la creșterea gradului de sensibilizare cu privire la indicatorii privind amenințările cibernetice și la recomandările privind măsurile de atenuare, ENISA ar trebui să pună la dispoziția entităților care își desfășoară activitatea în sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555 un serviciu de alertă

timpurie. Astfel de alerte timpurii generice și voluntare ar trebui să fie în special în beneficiul IMM-urilor și ar trebui să fie furnizate într-un format prelucrabil automat pus la dispoziția publicului. În orice caz, un astfel de serviciu voluntar este separat de orice parteneriat public-privat pe care ENISA îl poate institui sau l-a instituit deja și nu are legătură cu acesta.

(33) Pentru a sprijini conștientizarea comună a situației în materie de securitate cibernetică la nivelul Uniunii, ENISA, în strânsă cooperare cu statele membre, ar trebui să elaboreze periodic un raport aprofundat asupra situației tehnice în materie de securitate cibernetică la nivelul UE referitor la incidente și amenințări cibernetice, pe baza informațiilor disponibile public, a propriei analize și a rapoartelor care i-au fost transmise de echipele CSIRT ale statelor membre sau de punctele unice de contact naționale privind securitatea rețelelor și a sistemelor informatice („puncte unice de contact") prevăzute în Directiva (UE) 2022/2555, atât în mod voluntar, cât și de Europol și CERT-UE. Raportul respectiv ar trebui pus la dispoziția Consiliului, a Serviciului European de Acțiune Externă, a EU-CyCLONe, a rețelei CSIRT, a Comisiei și a Europol.

(34) Pentru a spori conștientizarea comună a situației în ceea ce privește peisajul amenințărilor și incidentelor cibernetice în rândul părților interesate, ENISA ar trebui să analizeze tendințele amenințărilor și incidentelor cibernetice. Aceasta ar trebui să includă o analiză periodică care să abordeze sectoarele cu o importanță critică ridicată și alte sectoare critice enumerate în anexele I și II la Directiva (UE) 2022/2555, inclusiv sectorul asistenței medicale, al energiei și al transporturilor. O astfel de analiză ar trebui să includă nivelurile de maturitate ale sectoarelor și să identifice, printre altele, posibilele provocări specifice unui anumit sector. După caz și pentru a identifica efectele asupra lanțului de aprovizionare, analiza ar trebui să evidențieze amenințările cibernetice și tendințele legate de categoriile de produse care intră sub incidența Regulamentului (UE) 2024/2847. ENISA ar trebui să dezvolte expertiză în domeniul securității cibernetice a infrastructurilor și al dependențelor critice ale acestora de lanțul de aprovizionare, în special pentru a sprijini sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555 și punerea în aplicare a Regulamentului (UE) 2024/2847. În acest scop, ENISA ar trebui, de asemenea, să coopereze, după caz, cu alte entități relevante ale Uniunii.

(35) În plus, pentru a înțelege mai bine provocările din domeniul securității cibernetice, ENISA trebuie să analizeze tehnologiile actuale și emergente și să furnizeze evaluări tematice specifice cu privire la impactul societal, juridic, economic și de reglementare preconizat al inovațiilor tehnologice asupra securității cibernetice. Pentru a asigura un acces mai ușor al publicului la informațiile privind riscurile în materie de securitate cibernetică și posibilele măsuri corective, ENISA poate furniza informații relevante pe site-ul său web, într-un mod ușor de utilizat și bine structurat.

(36) Rolul consolidat al ENISA în promovarea conștientizării situației, în analizarea amenințărilor și în furnizarea de consiliere tehnică va contribui la intensificarea eforturilor colective în materie de securitate cibernetică în ceea ce privește produsele cu elemente digitale și va sprijini punerea în aplicare a Regulamentului (UE) 2024/2847. În conformitate cu Regulamentul (UE) 2024/2847, ENISA poate propune autorităților de supraveghere a pieței activități comune de verificare a conformității produselor cu elemente digitale și poate identifica categoriile de produse cu elemente digitale pentru care pot fi organizate acțiuni de verificare. Informațiile care decurg din analiza amenințărilor cibernetice și din alertele timpurii ar trebui să consolideze sprijinul pe care ENISA îl oferă autorităților respective și să contribuie la o aplicare

eficace a Regulamentului (UE) 2024/2847 pentru a preveni efectele atacurilor cibernetice asupra lanțului de aprovizionare de pe piața internă și pentru a spori gradul general de pregătire al Uniunii.

(37) Atacurile de tip ransomware reprezintă o amenințare majoră la adresa securității cibernetice a Uniunii. Pentru a stimula securitatea cibernetică a Uniunii și pentru a combate atacurile de tip ransomware, ENISA ar trebui să dezvolte capabilități de conștientizare a situației și de sprijin pentru răspunsul la incidente și redresarea în urma acestora. Atunci când acordă asistență entităților esențiale și entităților importante individuale să răspundă la un atac de tip ransomware și să se redreseze în urma acestuia, ENISA ar trebui să coopereze îndeaproape cu Europol și cu echipele CSIRT sau cu autoritățile competente, după caz, valorificând astfel experiența dobândită de Europol în combaterea criminalității de tip ransomware. O astfel de asistență ar trebui să completeze activitățile echipelor CSIRT de sprijinire a răspunsului la incidente. Pentru a realiza sinergii în activitatea sa de combatere a atacurilor de tip ransomware, ENISA ar trebui să înființeze un serviciu de asistență și, în acest scop, ar putea pune în comun capacitățile relevante și serviciile de contracarare a atacurilor de tip ransomware și ar putea pune la dispoziție informații, orientări și instrumente ușor accesibile care pot ajuta entitățile esențiale și entitățile importante să răspundă la un incident de tip ransomware și să se redreseze în urma acestuia.

(38) ENISA ar trebui să ofere expertiză tehnică și sprijin Comisiei în elaborarea unui program anual continuu de exerciții de securitate cibernetică la nivelul Uniunii, în conformitate cu Recomandarea privind Planul de acțiune în materie de securitate cibernetică, pentru a se pregăti pentru crizele cibernetice, pentru a testa nivelul de securitate cibernetică al entităților care participă la astfel de exerciții și pentru a reduce la minimum duplicarea eforturilor. ENISA ar trebui, de exemplu, să ofere consiliere cu privire la tipurile adecvate de exerciții, cum ar fi simulările teoretice, hibride sau live integral, precum și cu privire la obiective, scenarii și participare.

(39) Accesul la informații corecte și în timp util cu privire la vulnerabilități și o gestionare solidă a vulnerabilităților sunt imperative pentru asigurarea unui nivel ridicat de securitate cibernetică pe piața internă. Din acest motiv, ENISA ar trebui să mențină o bază de date europeană a vulnerabilităților în temeiul Directivei (UE) 2022/2555 și să creeze o capacitate comună a Uniunii de servicii de gestionare a vulnerabilităților, asigurând un nivel rezilient și sustenabil al serviciilor și reducând riscul de perturbări. În acest scop, ENISA ar trebui să exploreze posibilitățile de aprofundare a cooperării structurate cu programe, registre sau baze de date similare cu baza de date europeană a vulnerabilităților, pentru a evita suprapunerea eforturilor și pentru a urmări complementaritatea la nivel internațional, după caz. În plus, ENISA ar trebui să sprijine divulgarea coordonată multipartită a vulnerabilităților la nivelul Uniunii și să furnizeze servicii cu valoare adăugată, cum ar fi avertismente în materie de vulnerabilitate, punctaje de gravitate și liste de produse, precum și să furnizeze un catalog european consolidat al vulnerabilităților exploatate cunoscute, pentru a ajuta entitățile în gestionarea vulnerabilităților.

(40) Rolul ENISA în dezvoltarea ECCF ar trebui să fie un aspect-cheie al mandatului său. ENISA ar trebui să își furnizeze expertiza tehnică pe parcursul întregului ciclu de viață al sistemelor europene de certificare a securității cibernetice. În vederea unui viitor sistem, ENISA ar trebui să identifice standardele sau specificațiile tehnice existente care pot sta la baza unui astfel de sistem și, după caz, să elaboreze ea însăși specificații tehnice la care se poate face trimitere în cadrul unui sistem. ENISA ar trebui să fie

responsabilă de pregătirea propunerilor de sisteme în urma unei solicitări în acest sens din partea Comisiei. Pentru sistemele deja existente, ENISA ar trebui să fie responsabilă de întreținerea acestora. În acest sens, ENISA ar trebui să contribuie la crearea și dezvoltarea unui ecosistem de certificare în care să se solicite feedback din partea statelor membre și a părților interesate din sectorul privat, iar capacitățile lor de certificare să fie consolidate. Aceasta ar trebui să includă, de asemenea, utilizarea unui site dedicat certificării, unde informațiile relevante referitoare la sistemele adoptate, inclusiv certificatele și declarațiile de conformitate, să fie accesibile în mod liber și public.

(41) Pentru a sprijini punerea în aplicare a legislației relevante a Uniunii, ENISA ar trebui să modeleze stadiul actual al tehnologiei în materie de securitate cibernetică prin furnizarea de specificații tehnice pentru a sprijini punerea în aplicare a legislației relevante a Uniunii, inclusiv având în vedere potențiala menționare a acestora în sistemele europene de certificare a securității cibernetice. ENISA ar trebui, de asemenea, să monitorizeze crearea și evoluția standardelor de către organismele de standardizare relevante în vederea urmăririi tendințelor în materie de standardizare la nivel european și mondial și, ori de câte ori este necesar, să modeleze aceste standarde prin participarea, inclusiv prin contribuții de redactare, și prin asumarea rolului de lider în activitățile organizațiilor de standardizare. În acest sens, ENISA ar trebui să rămână imparțială. De exemplu, ar putea exista situații în care ENISA ar trebui să se retragă din activitățile relevante ale organismelor de standardizare dacă i se solicită ENISA să evalueze standardele europene care au fost solicitate de Comisie în sprijinul legislației Uniunii. ENISA nu ar trebui să contribuie la elaborarea standardelor pe care este responsabilă să le evalueze.

(42) Pentru a sprijini punerea în aplicare a politicilor Uniunii și pregătirea potențialelor activități de standardizare, ENISA ar trebui să contribuie la dezvoltarea și evaluarea algoritmilor criptografici, în special în domeniul criptografiei post-cuantice. În acest context, la cererea Comisiei și sub rezerva unui acord de contribuție, astfel cum este definit în Regulamentul (UE, Euratom) 2024/2509 al Parlamentului European și al Consiliului[50], ENISA poate institui un proces de solicitare și evaluare a algoritmilor pentru algoritmii criptografici de către părțile interesate relevante, în special de către comunitățile criptografice, academice și de cercetare, precum și de către producători, echipele CSIRT, autoritățile naționale de certificare a securității cibernetice și autoritățile competente în temeiul Directivei (UE) 2022/2555. În cazul în care contribuie la instituirea unor astfel de procese, ENISA ar trebui să promoveze colaborarea dintre părțile interesate relevante și să pună în aplicare aspectele organizaționale. Procesul ar trebui să fie formal, deschis, transparent și incluziv, incluzând consultarea părților interesate relevante cu privire la proiectele de cerințe minime, precum și procesul de evaluare și criteriile de evaluare, în special în ceea ce privește securitatea și efectuarea evaluărilor.

(43) Pentru a sprijini punerea în aplicare a activităților de evaluare a conformității în cadrul sistemelor europene de certificare a securității cibernetice și al altor acte legislative relevante ale Uniunii, ENISA poate furniza instrumente de testare tehnică relevante pentru a sprijini statele membre, întreprinderile și organismele de evaluare a conformității în activitățile de evaluare. Astfel de instrumente ar trebui să vizeze

[50] Regulamentul (UE, Euratom) 2024/2509 al Parlamentului European și al Consiliului din 23 septembrie 2024 privind normele financiare aplicabile bugetului general al Uniunii (JO L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

crearea de sinergii la nivelul Uniunii și o funcționare eficientă a procedurilor de evaluare a conformității pentru a răspunde nevoilor statelor membre și ale pieței. Astfel de nevoi pot apărea, de exemplu, în domeniul securității de la stadiul conceperii pentru a sprijini întreprinderile, inclusiv întreprinderile mici și mijlocii, în eforturile lor de punere în aplicare în contextul Regulamentului 2024/2847. În acest context, ENISA ar trebui să perceapă taxe pentru a acoperi costurile relevante legate de instituirea, proiectarea, dezvoltarea, întreținerea și actualizarea capacităților software și hardware necesare pentru astfel de instrumente de testare.

(44) Pentru a sprijini statele membre în eforturile lor de a aborda deficitul de profesioniști în domeniul securității cibernetice și nevoia tot mai mare de o forță de muncă calificată, diversă, inclusiv în ceea ce privește echilibrul de gen, și agilă, precum și pentru a permite mobilitatea forței de muncă și pregătirea în toate statele membre, ENISA ar trebui să se bazeze pe principiile și activitatea inițiate în cadrul Academiei de competențe în materie de securitate cibernetică. În special, ENISA ar trebui să instituie Cadrul european de competențe în materie de securitate cibernetică („ECSF”) ca un cadru comun privind profilurile rolurilor profesionale în materie de securitate cibernetică. ENISA ar trebui să sprijine în continuare statele membre în abordarea disparităților de gen în rolurile în materie de securitate cibernetică. Această abordare este în concordanță cu viziunea prezentată în Comunicarea Comisiei privind uniunea competențelor și ar contribui la obiectivele acesteia. Ar trebui explorată în continuare o etichetă de calitate pentru atestările europene individuale de competențe în materie de securitate cibernetică.

(45) ECSF ar trebui să fie un instrument practic și flexibil care să fie utilizat în mod voluntar și care să ofere o înțelegere și o terminologie comună a rolurilor relevante și a sarcinilor, competențelor și cunoștințelor asociate necesare în principal în rolurile în materie de securitate cibernetică, cu scopul de a sprijini identificarea seturilor de competențe critice, inclusiv a competențelor transversale, necesare pentru forța de muncă și de a permite furnizorilor de servicii educaționale, inclusiv întreprinderilor, instituțiilor de învățământ superior sau furnizorilor de educație și formare profesională, să conceapă programe și să ajute factorii de decizie să dezvolte inițiative pentru a aborda lacunele în materie de competențe. Având potențialul de a fi utilizat drept cadru de referință pentru recunoașterea competențelor, acesta ar trebui, de asemenea, să fie interoperabil cu Clasificarea europeană a aptitudinilor și ocupațiilor (ESCO), pentru a sprijini departamentele de resurse umane să înțeleagă cerințele privind planificarea resurselor, recrutarea și dezvoltarea carierei în sprijinul nevoilor în materie de securitate cibernetică. În timp ce Cadrul european al competențelor digitale pentru cetățeni 3.0 descrie cunoștințele, aptitudinile și atitudinile care sunt necesare pentru a fi competent din punct de vedere digital pentru viața de zi cu zi, participarea în societate, muncă și învățare și care pot fi utilizate atât de adulți, cât și de copii, ECSF oferă un cadru simplu de identificare a rolurilor în materie de securitate cibernetică și a sarcinilor, cunoștințelor și competențelor asociate necesare pentru îndeplinirea acestora. În acest sens, acesta se adresează unui public specializat în domeniul securității cibernetice, de la profesioniști în domeniul securității cibernetice, de fapt sau potențiali, instituții de învățământ, până la angajatori. ECSF ar trebui, de asemenea, să sprijine dezvoltarea atestărilor europene individuale de competențe în materie de securitate cibernetică, fiind instrumentul-cheie utilizat pentru dezvoltarea sistemelor, permițând apariția unor noi actori pe piață și sprijinind concurența pe piață într-un cadru comun. ECSF ar trebui evaluat și actualizat periodic pentru a se asigura că reflectă în mod adecvat nevoile pieței forței de muncă în materie de securitate cibernetică și evoluțiile tehnologice și în materie de politici. ENISA ar trebui să

sprijine adoptarea ECSF de către statele membre și entitățile Uniunii și în cadrul acestora și să ofere sprijin adecvat în cazul în care este necesară o astfel de asistență.

(46) Competențele și calificările în materie de securitate cibernetică ar trebui să devină comparabile, transparente și de încredere în întreaga piață internă. În acest scop, atestările europene individuale de competențe în materie de securitate cibernetică[51] ar trebui să sprijine angajatorii, inclusiv IMM-urile și întreprinderile nou-înființate, să recruteze profesioniști existenți sau potențiali în materie de securitate cibernetică în mod eficace în interiorul statelor membre și între acestea, în conformitate cu obiectivele stabilite în Comunicarea privind uniunea competențelor. Pentru a asigura o punere în aplicare coerentă în toate statele membre, atestările europene individuale de competențe în materie de securitate cibernetică ar trebui să se bazeze pe o înțelegere comună, la nivelul Uniunii, a competențelor necesare pentru îndeplinirea acestor obiective și ar trebui să fie furnizate de furnizori autorizați de ENISA pe baza unui set comun de criterii. Această abordare ar trebui să fie în concordanță cu obiectivele viitoarei Inițiative privind portabilitatea competențelor și să contribuie la acestea.

(47) Dezvoltarea sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică ar trebui să vizeze completarea acțiunilor statelor membre, oferind autorităților publice și actorilor economici posibilitatea de a utiliza un mecanism european de atestare, în conformitate cu competența de sprijin a Uniunii în domeniul educației și formării profesionale, astfel cum se menționează la articolul 6 litera (e), la articolul 165 alineatul (1) și la articolul 166 alineatul (1) din TFUE. Împreună cu activitatea Academiei de competențe în materie de securitate cibernetică, sistemele pot reprezenta, de asemenea, baza pentru programele de învățământ superior, cum ar fi diplomele europene sectoriale, și pentru dezvoltarea microcertificatelor. Prin urmare, sistemele europene de atestare individuală a securității cibernetice nu ar trebui să vizeze armonizarea actelor cu putere de lege și a normelor administrative din statele membre, ci mai degrabă să fie considerate un factor favorizant și o oportunitate pe care statele membre și actorii economici ar putea dori să o adopte și să o promoveze.

(48) ENISA ar trebui să se asigure că sistemele europene de atestare individuală a competențelor în materie de securitate cibernetică rămân apropiate de nevoile pieței și se bazează pe experiența furnizorilor publici și privați de certificări individuale, inclusiv a statelor membre, a instituțiilor de învățământ superior, a instituțiilor de educație și formare profesională și a întreprinderilor. ENISA ar trebui să consulte Comisia cu privire la stabilirea priorităților sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică, ținând seama în mod corespunzător de punerea în aplicare a politicilor și de nevoile pieței.

(49) Pentru a asigura alinierea dintre ECSF și sisteme, revizuirea unui profil de rol al ECSF ar trebui să declanșeze automat o evaluare a adecvării sistemului sau sistemelor europene individuale asociate de atestare a competențelor în materie de securitate cibernetică, care poate conduce la revizuirea acestora.

---

[51] Atestările europene individuale de competențe în materie de securitate cibernetică ar trebui înțelese ca urmând o abordare similară cu ceea ce piața recunoaște drept „certificări de securitate cibernetică”. Cu toate acestea, pentru a evita confuzia în ceea ce privește cadrul european de certificare a securității cibernetice, se preferă expresia „atestare”, utilizată deja în comunicarea privind Academia de competențe în materie de securitate cibernetică.

(50) Având în vedere diversitatea profilurilor rolurilor în materie de securitate cibernetică și a sarcinilor, competențelor și cunoștințelor asociate, este posibil ca evaluarea persoanelor și metodele de evaluare să trebuiască să fie adaptate în fiecare sistem european de atestare individuală a competențelor în materie de securitate cibernetică. Fiecare sistem ar trebui să se asigure că evaluarea competențelor necesare ale unei persoane în ceea ce privește rezultatele învățării, inclusiv, după caz, evaluarea nivelului de competență, este evaluată în mod sistematic în raport cu un profil de rol ECSF sau cu un subset al acestuia. Metodele de evaluare pot include elemente precum testarea cunoștințelor teoretice, examinarea practică, condițiile prealabile și evaluarea *inter pares*. Experiența persoanelor ar trebui luată în considerare în mod corespunzător.

(51) Pentru a asigura o punere în aplicare coerentă a sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică, în special în ceea ce privește evaluarea persoanelor, ENISA ar trebui să ofere formare obligatorie personalului responsabil cu efectuarea evaluării persoanelor. Acest personal ar trebui să aibă experiență în domeniul securității cibernetice, care ar putea fi demonstrată prin deținerea unui atestat european individual de competențe în materie de securitate cibernetică pentru profilul de rol pentru care efectuează evaluarea și la un nivel de competență cel puțin echivalent cu cel al persoanelor pe care le evaluează.

(52) Rolul furnizorilor de atestate autorizați este de a atesta cunoștințele și competențele unei persoane pentru a putea îndeplini unul dintre rolurile ECSF și pentru a oferi asigurări angajatorilor din întreaga Uniune. Întrucât angajatorii care exploatează infrastructura critică a Uniunii ar analiza, de asemenea, asigurarea calității aptitudinilor și competențelor persoanelor care dobândesc atestarea individuală europeană a competențelor în materie de securitate cibernetică, furnizorii autorizați care atestă nivelul aptitudinilor și competențelor ar trebui să fie de încredere din punctul de vedere al securității cibernetice și nu ar trebui să facă obiectul influenței nejustificate a unei țări terțe care poate genera motive de îngrijorare în materie de securitate cibernetică. Prin urmare, entitățile stabilite într-o țară terță care prezintă motive de îngrijorare în materie de securitate cibernetică desemnate în conformitate cu prezentul regulament sau controlate de o astfel de țară terță, de o entitate stabilită într-o astfel de țară terță sau de un resortisant al unei astfel de țări terțe (furnizori cu grad ridicat de risc) în conformitate cu prezentul regulament nu ar trebui să fie eligibile pentru a deveni furnizori autorizați de atestate europene individuale de competențe în materie de securitate cibernetică în temeiul titlului II secțiunea 4.

(53) Pentru a se asigura că persoanele care dețin un atestat european al competențelor în materie de securitate cibernetică îl pot utiliza și comunica cu ușurință și că un astfel de atestat poate fi utilizat în toate statele membre, furnizorii de atestate autorizați ar trebui să se asigure că atestările electronice ale atestatelor europene individuale de competențe în materie de securitate cibernetică sunt eliberate în portofelul european pentru identitatea digitală (portofelul EUDI) instituit prin Regulamentul (UE) nr. 910/2014, la cererea persoanei în cauză. Furnizorii de atestate autorizați ar trebui considerați prestatori de servicii de încredere și ar trebui să facă obiectul regimului de supraveghere și de răspundere prevăzut în Regulamentul (UE) nr. 910/2014. Sistemul de atestare a atributelor utilizat în temeiul Regulamentului de punere în aplicare

(UE) 2025/1569 al Comisiei[52] ar trebui înregistrat în catalogul sistemelor de atestare a atributelor prevăzut în regulamentul de punere în aplicare respectiv.

(54) Pentru a contribui la dezvoltarea forței de muncă din domeniul securității cibernetice și la portabilitatea competențelor în întreaga Uniune, ENISA ar trebui să pună la dispoziția publicului, prin intermediul unui site dedicat, sistemele europene de atestare individuală a competențelor în materie de securitate cibernetică și lista furnizorilor de atestate autorizați.

(55) ENISA ar trebui să fie administrată și să funcționeze ținând seama de principiile Abordării comune referitoare la agențiile descentralizate ale Uniunii, adoptate la 19 iulie 2012 de către Parlamentul European, Consiliu și Comisie[53]. Recomandările cuprinse în abordarea comună ar trebui să se reflecte, după caz, în programele de activitate, evaluările și practicile administrative și de raportare ale ENISA.

(56) Astfel încât consiliul de administrație să își îndeplinească funcțiile în mod eficace, în special în ceea ce privește orientarea generală a activităților ENISA și stabilirea priorităților sale strategice, este esențial ca acesta să fie format din reprezentanți la nivel înalt ai statelor membre și ai Comisiei. În acest scop, fiecare stat membru ar trebui să numească șeful unei autorități naționale competente a statului membru respectiv responsabile cu securitatea cibernetică, desemnată în temeiul articolului 8 alineatul (1) din Directiva (UE) 2022/2555, în calitate de membru al consiliului de administrație.

(57) Pentru a se asigura că supleanții din consiliul de administrație își pot îndeplini rolurile în mod adecvat, statele membre ar trebui să numească supleanți care să aibă expertiza și experiența profesională corespunzătoare. Comisia și statele membre, în ceea ce privește supleanții, ar trebui să depună eforturi pentru a obține o reprezentare echilibrată a bărbaților și femeilor în consiliul de administrație și ar trebui să limiteze rotația acestora pentru a asigura continuitatea activității consiliului de administrație.

(58) Pentru a permite ENISA să își îndeplinească misiunea în mod eficace, consiliul de administrație, alcătuit din reprezentanți ai statelor membre și ai Comisiei, ar trebui să stabilească direcția generală a operațiunilor ENISA, inclusiv prioritățile sale strategice, și să se asigure că aceasta își îndeplinește sarcinile în conformitate cu prezentul regulament. Consiliului de administrație ar trebui să i se încredințeze competențele necesare pentru a stabili și a verifica execuția bugetului, pentru a adopta norme financiare adecvate, pentru a stabili proceduri de lucru transparente pentru procesul decizional al ENISA, pentru a adopta documentul unic de programare al ENISA, pentru a-și adopta propriul regulament de procedură, pentru a numi directorul executiv, pentru a decide cu privire la prelungirea și încetarea mandatului directorului executiv și pentru a decide dacă să creeze o funcție de director executiv adjunct și, în cazul creării unei astfel de funcții, cu privire la numirea acestuia, precum și cu privire la prelungirea și încetarea mandatului său. Orice persoană care exercită o funcție executivă în cadrul ENISA ar trebui, prin urmare, să fie numită de consiliul de administrație. Consiliul de administrație ar trebui, de asemenea, să fie responsabil de

---

52 Regulamentul de punere în aplicare - UE - 2025/1569.

53 Abordarea comună, anexată la Declarația comună a Parlamentului European, a Consiliului UE și a Comisiei Europene privind agențiile descentralizate, adoptată la 19 iulie 2012 și disponibilă la adresa: https://european-union.europa.eu/document/download/d4199ff4-1e3d-45e6-af7e-90cf1a7b10bc_en?filename=joint_statement_on_decentralised_agencies_en.pdf.

numirea sau demiterea membrilor comisiei pentru soluționarea contestațiilor, precum și de stabilirea unor norme de prevenire sau gestionare a conflictelor de interese în acest sens.

(59) Pentru a contribui la asigurarea faptului că ENISA își stabilește prioritățile strategice și le actualizează, consiliul de administrație ar trebui să organizeze cel puțin o reuniune pe an dedicată priorităților strategice ale ENISA. Pentru a se asigura că reuniunile consiliului de administrație sunt eficace și bine informate, consiliul de administrație poate invita la reuniunile sale orice persoană a cărei opinie ar putea fi pertinentă și de interes pentru subiectele discutate, pentru a oferi informații, expertiză sau consiliere. O astfel de persoană ar fi un observator ad-hoc fără drept de vot.

(60) Consiliul de administrație ar trebui să adopte decizii cu majoritatea absolută a membrilor săi cu drept de vot, cu excepția cazului în care se prevede altfel în prezentul regulament. Având în vedere importanța aspectelor legate de buget și de resursele umane, în special a aspectelor legate de bugetul anual, de raportul anual de activitate, de strategia antifraudă, de normele de punere în aplicare a Statutului funcționarilor, de numirea directorului executiv, a directorului executiv adjunct și a contabilului, de acțiunile întreprinse în urma constatărilor Oficiului European de Luptă Antifraudă (OLAF) și ale Parchetului European (EPPO), precum și de adoptarea normelor financiare ale ENISA, consiliul de administrație ar trebui să adopte astfel de decizii numai dacă reprezentantul Comisiei votează pozitiv. În scopul luării unei decizii cu privire la adoptarea unui document unic de programare final după luarea în considerare a avizului Comisiei, ar trebui să se solicite un vot pozitiv al reprezentantului Comisiei numai cu privire la elementele deciziei care nu au legătură cu programul de lucru anual și multianual al ENISA.

(61) Comitetul executiv ar trebui să contribuie la funcționarea eficace a consiliului de administrație. În cadrul lucrărilor sale pregătitoare legate de deciziile consiliului de administrație, comitetul executiv ar trebui să examineze în detaliu informațiile relevante, să analizeze opțiunile disponibile și să ofere consiliere și soluții pentru pregătirea deciziilor relevante ale consiliului de administrație. De asemenea, acesta ar trebui să îl asiste și să îl consilieze pe directorul executiv în punerea în aplicare a deciziilor consiliului de administrație.

(62) Pentru buna funcționare a ENISA este necesar ca numirea directorului executiv să fie făcută pe baza meritelor și aptitudinilor sale administrative și manageriale atestate, precum și a competenței și experienței relevante în domeniul securității cibernetice. Directorul executiv ar trebui să își ducă la îndeplinire atribuțiile în deplină independență. Consiliul de administrație ar trebui să numească directorul executiv din lista de candidați pregătită de Comisie, în urma unei proceduri deschise și transparente care respectă principiul echilibrului de gen.

(63) Directorul executiv ar trebui să elaboreze o propunere privind documentul unic de programare al ENISA, după consultări prealabile cu Comisia, și să ia toate măsurile necesare pentru a asigura punerea în aplicare corespunzătoare a documentului unic de programare respectiv. Directorul executiv ar trebui să întocmească un raport anual cuprinzând și punerea în aplicare a programului anual de activitate al ENISA, care să fie prezentat consiliului de administrație, să elaboreze un proiect de situație a estimărilor de venituri și cheltuieli ale ENISA și să execute bugetul. În plus, directorul executiv ar trebui să aibă opțiunea de a înființa grupuri de lucru ad-hoc pentru a aborda aspecte specifice, în special de natură științifică, tehnică, juridică sau socioeconomică. Se consideră drept necesară instituirea unui grup de lucru ad-hoc,

mai ales în legătură cu pregătirea unei anumite propuneri de sistem european de certificare a securității cibernetice („propunere de sistem”). Înființarea unui grup de lucru ad-hoc ar putea fi, de asemenea, necesară pentru activitățile de întreținere legate de anumite sisteme europene de certificare a securității cibernetice adoptate. De asemenea, ar trebui înființate grupuri de lucru ad-hoc pentru a dezvolta și a menține sisteme europene de atestare individuală a competențelor în materie de securitate cibernetică și pentru a asista agenția în guvernanța, punerea în aplicare și evoluția ECSF. Directorul executiv ar trebui să se asigure că selecționarea membrilor grupurilor de lucru ad-hoc se realizează în conformitate cu cele mai înalte standarde de competență, urmărindu-se să se asigure o reprezentare echilibrată din perspectiva genului și corespunzătoare, în funcție de problemele specifice – între administrațiile publice ale statelor membre, entitățile Uniunii și sectorul privat, inclusiv industria, utilizatorii și experții universitari în domeniul securității rețelelor și a informațiilor, precum și experții universitari în produse cu elemente digitale.

(64) Consiliul de administrație poate decide să creeze o funcție de director executiv adjunct care să îl asiste pe directorul executiv, în cazul în care consiliul de administrație consideră că o astfel de funcție este necesară pentru a asigura sau a menține buna funcționare a ENISA. Atunci când decide dacă să creeze sau nu funcția respectivă, consiliul de administrație poate ține seama de avizul directorului executiv.

(65) ENISA ar trebui să aibă un grup consultativ pentru a asigura un dialog periodic cu sectorul privat, cu organizațiile de consumatori și cu alte părți interesate relevante. Grupul consultativ al ENISA, instituit de consiliul de administrație la propunerea directorului executiv, ar trebui să se concentreze pe probleme relevante pentru părțile interesate și să le aducă în atenția ENISA. Grupul consultativ al ENISA ar trebui să fie consultat în special în legătură cu proiectul de program anual de activitate al ENISA. Componența Grupului consultativ al ENISA și atribuțiile încredințate acestuia ar trebui să asigure faptul că părțile interesate sunt reprezentate într-o măsură suficientă în ceea ce privește activitatea ENISA. Reprezentanții autorităților naționale și ale Uniunii responsabile de aplicarea legii, de protecția datelor și de supravegherea pieței ar trebui să fie eligibili pentru a fi reprezentați în cadrul grupului consultativ al ENISA.

(66) Solicitanții care doresc să devină furnizori de atestate autorizați sau să își reînnoiască autorizația ar trebui să aibă acces la căile de atac necesare în cazul în care sunt afectați de deciziile luate de ENISA. Prin urmare, ar trebui instituit un mecanism de apel corespunzător, astfel încât deciziile conexe ale ENISA să poată fi contestate în fața unei comisii pentru soluționarea contestațiilor, ale cărei decizii să poată face obiectul controlului jurisdicțional de către Curtea de Justiție a Uniunii Europene, în conformitate cu tratatele. Cerința de a epuiza procedura de soluționare a contestațiilor în cadrul ENISA înainte de a introduce o acțiune în fața Curții de Justiție a Uniunii Europene se aplică numai persoanelor care au calitate procesuală în fața comisiei de soluționare a contestațiilor.

(67) Pentru a garanta autonomia și independența deplină a ENISA și pentru a-i permite să își îndeplinească sarcinile, ENISA ar trebui să beneficieze de un buget suficient și autonom, finanțat în principal dintr-o contribuție din partea Uniunii, dar și din contribuții din partea țărilor terțe care participă la activitatea ENISA, precum și din taxele plătite de furnizorii de atestate autorizați și de organismele de evaluare a conformității care participă la sisteme și care emit certificate europene de securitate cibernetică și declarații de conformitate UE. Statul membru gazdă și oricare alt stat membru ar trebui să poată contribui în mod voluntar la bugetul ENISA. Nicio

contribuție financiară sau în natură primită de ENISA din partea statelor membre, a țărilor terțe sau a altor entități sau persoane nu ar trebui să îi compromită independența și imparțialitatea. Procedura bugetară a Uniunii ar trebui să se aplice în ceea ce privește contribuția Uniunii și alte eventuale subvenții de la bugetul general al Uniunii. Curtea de Conturi ar trebui să auditeze conturile ENISA pentru a asigura transparența și responsabilitatea. Pentru a permite agenției să participe la toate proiectele viitoare de interes, ar trebui să i se acorde posibilitatea de a beneficia de granturi.

(68) Pentru a asigura capacitatea ENISA de a răspunde cererii de activități pe care le desfășoară, în special în ceea ce privește deciziile de autorizare a furnizorilor să furnizeze atestate europene individuale de competențe în materie de securitate cibernetică și în ceea ce privește întreținerea sistemelor europene de certificare a securității cibernetice și a instrumentelor de testare, ENISA ar trebui să aibă competența de a percepe taxe. Taxele asociate prelucrării cererilor de a deveni furnizor de atestate autorizat ar trebui stabilite în mod corespunzător pentru a contribui în mod suficient la acoperirea costurilor estimate ale dezvoltării și menținerii sistemelor de atestare europeană individuală a competențelor în materie de securitate cibernetică și la evaluarea îndeplinirii și a continuării îndeplinirii cerințelor și obligațiilor de a deveni și de a rămâne furnizor de atestate autorizat. Taxele asociate costurilor de eliberare și reînnoire a autorizațiilor pentru furnizorii de atestate autorizați ar trebui să includă costurile asociate evaluărilor efectuate de ENISA sau sub supravegherea acesteia. Taxele asociate participării la sistemele europene de certificare a securității cibernetice și pentru eliberarea de certificate în cadrul acestor sisteme ar trebui să fie stabilite în mod corespunzător pentru a contribui în mod suficient la acoperirea costurilor estimate ale menținerii unor astfel de sisteme. Plata acestor taxe ar trebui să permită organismelor de evaluare a conformității notificate și, după caz, deținătorilor de certificate din cadrul unui sistem să participe la astfel de activități, precum și la activități relevante de consolidare a capacităților și de promovare pentru a promova schimbul de bune practici și pentru a încuraja adoptarea sistemelor și a soluțiilor certificate.

(69) Pentru a asigura proporționalitatea, transparența și securitatea juridică, taxele ar trebui stabilite într-un mod transparent și echitabil. Toate cheltuielile ENISA atribuite personalului implicat în activități care fac obiectul unor taxe, în special contribuția proporțională a angajatorului la sistemul de pensii, precum și costurile legate de comisia pentru soluționarea contestațiilor, ar trebui să se reflecte în costul respectiv. Taxele nu trebuie să conducă la impunerea unor sarcini financiare sau administrative inutile solicitanților. Pentru plata taxelor ar trebui stabilite termene rezonabile.

(70) Este necesar să se instituie un set de indicatori pentru a măsura volumul de muncă, eficacitatea și eficiența agenției în ceea ce privește activitățile finanțate prin taxe. Având în vedere acești indicatori, agenția ar trebui să își adapteze planificarea personalului și gestionarea resurselor legate de taxe pentru a putea răspunde în mod adecvat unei astfel de cereri și oricăror fluctuații ale veniturilor din taxe.

(71) Pentru a identifica și a gestiona corect riscul unui conflict de interese real sau perceput, ENISA ar trebui să dispună de norme privind prevenirea și gestionarea conflictelor de interese. De asemenea, ENISA ar trebui să aplice normele privind accesul la documente prevăzute în Regulamentul (CE) nr. 1049/2001 al Parlamentului

European și al Consiliului[54]. Prelucrarea datelor cu caracter personal de către ENISA ar trebui să intre sub incidența Regulamentului (UE) 2018/1725 al Parlamentului European și al Consiliului[55]. ENISA ar trebui să se conformeze dispozițiilor aplicabile entităților Uniunii, precum și dispozițiilor legislațiilor naționale privind gestionarea informațiilor, în special a informațiilor sensibile neclasificate și a informațiilor clasificate ale Uniunii Europene (IUEC).

(72) Atunci când își îndeplinește sarcinile, ENISA poate avea acces la informații sensibile, cum ar fi informațiile privind amenințările și incidentele cibernetice. Prin urmare, este esențial ca ENISA să păstreze confidențialitatea informațiilor pe care le gestionează. În special, în conformitate cu articolul 339 din Tratatul privind funcționarea Uniunii Europene (TFUE), funcționarii și alți agenți ai ENISA nu ar trebui să divulge nicio informație de tipul celor care fac obiectul obligației de păstrare a secretului profesional, în special informații despre întreprinderi, relațiile lor de afaceri sau componentele de cost, chiar și după încetarea atribuțiilor lor.

(73) Pentru a asigura îndeplinirea în totalitate a obiectivelor sale, ENISA ar trebui să colaboreze cu autoritățile de supraveghere relevante ale Uniunii și cu alte autorități competente din Uniune, cu entitățile relevante ale Uniunii, inclusiv CERT-UE, EC3 din cadrul Europol, ECCC, Agenția Europeană de Apărare (AEA), Agenția Uniunii Europene pentru Programul spațial (EUSPA), Organismul Autorităților Europene de Reglementare în Domeniul Comunicațiilor Electronice (OAREC), Agenția Europeană pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă (eu-LISA), Banca Centrală Europeană (BCE), Autoritatea Bancară Europeană (ABE), Comitetul european pentru protecția datelor, Agenția pentru Cooperarea Autorităților de Reglementare din Domeniul Energiei (ACER), Agenția Uniunii Europene pentru Siguranța Aviației (AESA) și orice altă entitate a Uniunii implicată în securitatea cibernetică. De asemenea, ENISA ar trebui să colaboreze cu autoritățile competente în temeiul Directivei (UE) 2022/2555, cu autoritățile de supraveghere a pieței și cu autoritățile care se ocupă de protecția datelor pentru a face schimb de know-how și de bune practici și ar trebui să ofere consiliere cu privire la aspectele legate de securitatea cibernetică care ar putea avea un impact asupra activității lor.

(74) Europol are un rol important în prevenirea și combaterea criminalității informatice, inclusiv a criminalității informatice legate de incidentele de securitate a rețelelor și a informațiilor. Pentru a crea sinergii între sarcinile respective ale fiecărei agenții, ENISA ar trebui să coopereze cu Europol, în special prin schimbul de informații cu privire la tendințele în ceea ce privește tehnicile, cererile și impactul atacurilor de tip ransomware. O astfel de cooperare poate consta, de asemenea, în identificarea celor mai frecvente tipuri de atac de tip ransomware care vizează entitățile enumerate în anexele I și II la Directiva (UE) 2022/2555 pentru a sprijini entitățile esențiale și importante în răspunsul la incidente și redresarea în urma acestora.

---

54 Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei (JO L 145, 31.5.2001, p. 43, ELI: http://data.europa.eu/eli/reg/2001/1049/oj).

55 Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(75) Pentru a sprijini cooperarea operațională și conștientizarea comună a situației în ceea ce privește amenințările și incidentele cibernetice, este esențial ca ENISA să coopereze cu părțile interesate și, în special, cu întreprinderile și organizațiile din sectorul privat, cu care ENISA poate institui parteneriate public-privat.

(76) Pentru a îndeplini în mod eficace obiectivele prezentate în prezentul regulament, ENISA poate colabora în special cu instituțiile academice care au inițiative de cercetare în domenii relevante și poate dezvolta canale adecvate pentru contribuții din partea organizațiilor consumatorilor și a altor organizații.

(77) Având în vedere că amenințările și incidentele cibernetice nu au frontiere, nivelul de securitate cibernetică și de pregătire al țărilor terțe poate avea un impact asupra entităților din Uniune. Prin urmare, ENISA ar trebui să fie în măsură să ofere activități de consolidare a capacităților, inclusiv formare, consolidarea capacităților, activități de înfrățire în țări terțe și, în special, activități adaptate de consolidare a capacităților pentru țările candidate la aderarea la Uniune sau pentru alte țări partenere, în conformitate cu prioritățile Uniunii. Astfel de activități ar trebui să se desfășoare în urma unei cereri specifice de a oferi sprijin adecvat, ținând seama de prioritățile Uniunii, și să fie puse în aplicare prin regimuri speciale, inclusiv prin acorduri de contribuție, astfel cum se menționează în Regulamentul (UE, Euratom) 2024/2509. Cadrul european de certificare a securității cibernetice urmărește să protejeze împotriva amenințărilor cibernetice, cum ar fi vulnerabilitățile în materie de securitate cibernetică exploatate în mod răuvoitor sau incidentele de securitate cibernetică care afectează funcționalitatea (proiectarea și funcționarea) produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate sau postura de securitate cibernetică a entităților. Axându-se pe riscurile tehnice legate de produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura de securitate cibernetică a entităților, ECCF ar trebui să completeze cadrul de securitate a lanțurilor de aprovizionare TIC, care urmărește să asigure o abordare armonizată la nivelul Uniunii pentru a aborda riscurile non-tehnice din sectoarele cu o importanță critică ridicată și din alte sectoare critice.

(78) Statele membre ar trebui să aibă posibilitatea de a recurge la certificarea europeană a securității cibernetice în contextul achizițiilor publice, în conformitate cu Directiva 2014/24/UE a Parlamentului European și a Consiliului[56].

(79) Pentru a facilita simplificarea conformității pentru entități, ECCF ar trebui să prevadă posibilitatea de a certifica postura de securitate cibernetică a acestora. Entitățile, în special cele care furnizează mai multe tipuri de servicii în mai multe state membre, se pot confrunta cu obligații diferite în materie de securitate cibernetică și de securitate a datelor în temeiul instrumentelor orizontale, cum ar fi Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului[57] și Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[58], precum și al instrumentelor sectoriale.

---

[56] Directiva 2014/24/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile publice și de abrogare a Directivei 2004/18/CE (JO L 94, 28.3.2014, p. 65, ELI: http://data.europa.eu/eli/dir/2014/24/oj).

[57] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

[58] Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a

Pentru a raționaliza punerea în aplicare a cadrului general de reglementare în materie de securitate cibernetică și pentru a facilita respectarea acestuia, ar trebui să fie posibil ca legislația Uniunii să prevadă posibilitatea ca entitățile să demonstreze conformitatea cu cerințele de gestionare a riscurilor în materie de securitate cibernetică prin intermediul unui certificat european de securitate cibernetică. Un sistem relevant ar putea contribui la raționalizarea cerințelor de conformitate care decurg din diferite instrumente de reglementare, fără a aduce atingere cerințelor lor specifice de certificare. Astfel de măsuri de simplificare au potențialul de a reduce sarcina administrativă, deblocând resurse pentru a consolida pregătirea operațională în materie de securitate cibernetică a entităților din sectoarele critice ale Uniunii.

(80) Certificarea europeană a cerințelor de gestionare a riscurilor în materie de securitate cibernetică elaborate în cadrul ECCF ar trebui să permită entităților să demonstreze conformitatea cu legislația relevantă a Uniunii în cazul în care un sistem acoperă cerințele juridice respective prevăzute într-un astfel de act și în cazul în care prevede acest lucru. Pe această bază, un act juridic al Uniunii poate prevedea, de asemenea, o prezumție de conformitate cu cerințele respective. Astfel de sisteme ar putea contribui la îmbunătățirea punerii în aplicare coerente a cerințelor de securitate cibernetică din legislația Uniunii pentru a asigura condiții de concurență echitabile între statele membre și pentru a reduce sarcina de asigurare a conformității.

(81) Cadrul european de certificare a securității cibernetice ar trebui să prevadă posibilitatea de a certifica procesele TIC, definite ca un set de activități desfășurate pentru proiectarea, dezvoltarea, livrarea sau întreținerea unui produs TIC sau a unui serviciu TIC. Un profil de protecție este un exemplu de proces TIC, astfel cum se specifică în Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei[59]. Un alt exemplu de proces TIC este setul de activități întreprinse de un producător pentru a proiecta și a dezvolta în condiții de siguranță un produs TIC, inclusiv măsurile fizice, logice, procedurale, de personal și alte măsuri de securitate care sunt necesare pentru a proteja confidențialitatea și integritatea proiectării și punerii în aplicare a unui produs TIC în mediul său de dezvoltare. Certificarea unor astfel de activități este adesea denumită „certificarea site-ului” în contextul unui proces de certificare în temeiul Regulamentului de punere în aplicare (UE) 2024/482 al Comisiei.

(82) Definiția serviciilor de securitate gestionate din prezentul regulament ar trebui să fie în concordanță cu cea a furnizorilor de servicii de securitate gestionate din Directiva (UE) 2022/2555. Serviciile respective constau în desfășurarea de activități legate de gestionarea riscurilor în materie de securitate cibernetică ale clienților lor sau în furnizarea de asistență pentru astfel de activități și au dobândit o importanță din ce în ce mai mare în prevenirea și atenuarea incidentelor. În consecință, furnizorii acestor servicii sunt considerați entități esențiale sau importante care aparțin unui sector cu o importanță critică ridicată în temeiul Directivei (UE) 2022/2555. Furnizorii de servicii de securitate gestionate în domenii precum răspunsul în caz de incidente, testele de penetrare, auditurile de securitate și consultanța joacă un rol deosebit de

---

Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (JO L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[59] Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei din 31 ianuarie 2024 de stabilire a normelor de aplicare a Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului în ceea ce privește adoptarea sistemului european de certificare a securității cibernetice bazat pe criterii comune (EUCC) (JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

important în sprijinirea entităților în eforturile lor de a preveni și de a detecta incidente, de a răspunde la acestea și de a se redresa după incidente. Cu toate acestea, și furnizorii de servicii de securitate gestionate au fost ținta atacurilor cibernetice și prezintă un risc deosebit din cauza integrării lor strânse în operațiunile clienților lor. Prin urmare, este necesar ca entitățile esențiale și entitățile importante, în înțelesul Directivei (UE) 2022/2555, să dea dovadă de o diligență sporită în selectarea furnizorilor de servicii de securitate gestionate.

(83) Sistemele europene de certificare a securității cibernetice sunt relevante pentru o comunitate largă de părți interesate, cum ar fi furnizorii de soluții TIC, organismele de evaluare a conformității și utilizatorii. Pentru a promova implicarea pe scară largă a părților interesate, Adunarea europeană pentru certificarea securității cibernetice („adunarea”) ar trebui organizată cel puțin o dată pe an, cu scopul de a încuraja colaborarea dintre Comisie, ENISA, statele membre și părțile interesate relevante. Acesta va juca un rol esențial în identificarea și abordarea noilor provocări în materie de securitate cibernetică și a priorităților strategice pentru certificare, precum și în asigurarea faptului că sistemele de certificare facilitează integrarea în condiții de siguranță a tehnologiilor digitale și sunt adecvate nevoilor utilizatorilor. Adunarea ar trebui să promoveze poziția de lider a Uniunii în activitățile de certificare și să susțină capacitatea cadrului de certificare de a oferi încredere întreprinderilor, autorităților publice și publicului.

(84) Comisia ar trebui să mențină un site dedicat pentru a asigura transparența prin publicarea de informații actualizate cu privire la progresele înregistrate în punerea în aplicare a ECCF. Site-ul ar trebui să includă informații referitoare la sistemele de certificare în curs de pregătire, priorități strategice pentru viitoarele sisteme de certificare, cereri adresate ENISA de a elabora propuneri de sisteme de certificare și informații privind adoptarea sistemelor de certificare. Site-ul Comisiei va completa site-ul ENISA privind sistemele europene de certificare a securității cibernetice, care ar trebui să ofere detalii cuprinzătoare cu privire la pregătirea tehnică a propunerilor de sisteme și la întreținerea sistemelor, punând accentul pe certificatele europene de securitate cibernetică eliberate și pe declarațiile de conformitate UE.

(85) Pentru a consolida dialogul dintre instituțiile Uniunii și pentru a contribui la un proces de consultare formal, deschis, transparent și favorabil incluziunii, Comisia ar trebui să țină seama, atunci când evaluează prezentul regulament, de elementele care decurg din opiniile exprimate de Parlamentul European și de Consiliu, precum și de Adunarea Europeană pentru Certificarea Securității Cibernetice.

(86) Studiile de fezabilitate efectuate de ENISA ar trebui să contribuie la pregătirea pentru planificarea și dezvoltarea sistemelor de certificare a securității cibernetice. Studiile ar trebui să includă perspectivele părților interesate relevante și să alinieze viitoarele sisteme de certificare la activitățile de cercetare, dezvoltare și evaluare tehnologică în curs, recunoscând, în special, contribuțiile inițiativelor de cercetare ale Uniunii și ale statelor membre. Aceste studii pot contribui la identificarea standardelor și a specificațiilor tehnice disponibile. Acestea ar trebui să fie efectuate la cererea Comisiei sau în conformitate cu prioritățile strategice ale Uniunii, pentru a se asigura că peisajul tehnologic în continuă evoluție și nevoile în materie de securitate cibernetică sunt abordate și reflectate în mod adecvat atunci când se solicită și se dezvoltă sisteme.

(87) Proiectarea sistemului propus și acoperirea de către acesta a obiectivelor și elementelor de securitate ar trebui să fie proporționale cu obiectul și domeniul de aplicare al obiectului certificării. De exemplu, un sistem de certificare a serviciilor de

cloud ar putea, prin urmare, să abordeze obiective de securitate care sunt relevante pentru serviciile TIC și pentru securitatea organizațională. Ca un alt exemplu, este probabil ca un obiectiv de securitate legat de neincluderea vulnerabilităților exploatabile cunoscute să nu fie relevant pentru certificarea proceselor TIC.

(88) Pentru a se asigura că sistemele europene de certificare a securității cibernetice sunt puse în aplicare în mod armonizat în toate statele membre, este necesar să se prevadă norme privind întreținerea sistemelor. Activitățile de întreținere sunt, de asemenea, necesare pentru a se asigura că sistemele și documentația lor justificativă rămân actualizate, în special într-un domeniu al securității cibernetice în care peisajul amenințărilor și tehnologiile evoluează în mod constant. Prin urmare, sistemele de certificare ar trebui să fie concepute și întreținute astfel încât să se evite riscul ca acestea să fie rapid depășite. Activitățile de întreținere ar trebui să implice, de regulă, elaborarea și actualizarea documentației justificative, inclusiv a specificațiilor tehnice și a orientărilor, precum și identificarea standardelor sau a specificațiilor tehnice care sunt relevante pentru sistem. Analiza funcționării sistemului, eventualele sale deficiențe și îmbunătățirile necesare ar trebui, de asemenea, să facă parte din activitățile de întreținere. În plus, activitățile de întreținere ar trebui să includă schimbul de informații între statele membre cu privire la punerea în aplicare a sistemelor și contribuțiile la mecanismele de revizuire *inter pares* și de evaluare *inter pares*.

(89) Având în vedere natura tehnică a activităților de întreținere, ENISA ar trebui să gestioneze aceste activități, în cooperare cu Comisia și cu sprijinul Grupului european pentru certificarea securității cibernetice (ECCG) și al subgrupului său relevant privind întreținerea. Instituirea subgrupului ECCG privind întreținerea permite colectarea de contribuții și informații tehnice din partea statelor membre în vederea armonizării abordărilor.

(90) Activitățile de întreținere ar trebui să implice interacțiuni cu grupurile relevante de părți interesate pentru a se asigura că sistemele rămân relevante pentru piață și actualizate, inclusiv prin partajarea și primirea de contribuții tehnice. Aceste grupuri de părți interesate pot fi organizații de standardizare, organisme de evaluare a conformității, vânzători, utilizatori, autorități publice sau asociații profesionale. Particularitățile fiecărui sistem, inclusiv forumurile tehnice și industriile corespunzătoare, implică faptul că ar trebui să fie posibilă colectarea contribuțiilor tehnice în moduri diferite de la un sistem la altul. Pentru unele sisteme, ENISA ar trebui să se poată baza pe un grup de lucru ad-hoc care să reunească experți din administrațiile publice ale statelor membre, din entitățile Uniunii și din sectorul privat. Contribuțiile tehnice ar putea proveni și de la ISAC sau de la organizațiile de standardizare. ENISA ar trebui să analizeze formatul cel mai adecvat pentru fiecare sistem și să includă o strategie de întreținere în fiecare propunere de sistem.

(91) Sistemele europene de certificare a securității cibernetice ar trebui să se bazeze pe standarde sau specificații tehnice, în special pentru definirea cerințelor de securitate și a metodologiilor de evaluare. ENISA ar trebui să aibă posibilitatea de a elabora specificații tehnice pentru a sprijini pregătirea și întreținerea sistemelor, în special în cazul în care livrabilele organizațiilor de standardizare lipsesc sau nu sunt adecvate pentru îndeplinirea obiectivelor sistemului. Ca parte a procesului de elaborare, ENISA ar trebui să fie sprijinită de ECCG și, după caz, de grupul de lucru ad-hoc instituit pentru sistemul relevant. De asemenea, ENISA ar trebui să solicite contribuții din partea grupurilor de părți interesate. În plus, ENISA ar trebui să ia în considerare acceptarea pe piață, precum și standardele europene și internaționale. Ținând seama de

calitatea specificațiilor tehnice și de obiectivele sistemului, Comisia ar trebui să aibă posibilitatea de a face trimitere la specificațiile tehnice elaborate de ENISA în cadrul unui sistem european de certificare a securității cibernetice.

(92) Specificațiile tehnice elaborate de ENISA și menționate într-un sistem ar trebui să fie puse la dispoziție pe site-ul ENISA privind sistemele europene de certificare a securității cibernetice, astfel încât să le poată accesa toate părțile interesate. Cu toate acestea, în unele cazuri specifice, publicarea pe site ar putea prezenta un risc pentru securitatea cibernetică a produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate certificate sau a posturii de securitate cibernetică a entităților și, prin extensie, pentru siguranța publică. De exemplu, specificațiile tehnice ar putea conține informații precise cu privire la noile căi de atac a căror disponibilitate publică ar permite actorilor răuvoitori să le utilizeze. Acest tip de informații ar trebui să fie distribuit în mod limitat, pe baza principiului necesității de a cunoaște, părților interesate relevante, cum ar fi autoritățile naționale de certificare a securității cibernetice, organismele de evaluare a conformității și vânzătorii certificați. Din cauza distribuției lor restrânse, aceste specificații tehnice nu ar trebui să fie menționate în sistemele europene de certificare a securității cibernetice și, prin urmare, ar trebui să aibă un caracter neobligatoriu.

(93) Sistemele de certificare a posturii de securitate cibernetică ar trebui să fie concepute într-un mod modular, pentru a permite demonstrarea conformității și a prezumției de conformitate cu cerințele de securitate cibernetică relevante prevăzute în alte acte legislative ale Uniunii, în cazul în care legislația respectivă prevede această posibilitate. Prin urmare, prezumția de conformitate cu cerințele acestor acte juridice va intra în vigoare ca o posibilă modalitate de a demonstra conformitatea numai dacă actele juridice respective permit o astfel de prezumție de conformitate. Detaliile unui astfel de sistem, și anume scopul, obiectivele sau elementele, vor fi, prin urmare, probabil diferite de cele ale altor sisteme. În special, ar trebui elaborate sisteme de certificare a posturii de securitate cibernetică a entităților pentru a asigura evaluarea continuă a conformității unei entități cu legislația Uniunii. Prin urmare, nu este necesar ca sistemele de certificare a posturii de securitate cibernetică să acopere toate elementele sistemelor europene de certificare a securității cibernetice, cum ar fi nivelurile de asigurare, iar acest lucru ar trebui să se reflecte în normele aplicabile sistemelor.

(94) Un cadru pentru certificarea posturii de securitate cibernetică în cadrul ECCF permite dezvoltarea unui sistem care permite entităților care furnizează servicii în mai multe state membre să demonstreze conformitatea cu obligațiile de gestionare a riscurilor în materie de securitate cibernetică prevăzute în Directiva 2022/2555 a Parlamentului European și a Consiliului. Pe această bază, având capacitatea de a demonstra conformitatea, entitățile pot beneficia de abordări mai coerente și mai puțin împovărătoare în materie de supraveghere în cadrul pieței interne. Dezvoltarea unui astfel de sistem de certificare ar trebui facilitată prin adoptarea unor acte de punere în aplicare în temeiul Directivei (UE) 2022/2555. Prin profiluri extinse, un sistem de certificare a posturii de securitate cibernetică poate demonstra conformitatea cu cerințele în cazul în care un stat membru a adoptat sau a menținut dispoziții care asigură un nivel mai ridicat de securitate cibernetică în conformitate cu Directiva (UE) 2022/2555. Pe această bază, o entitate care furnizează servicii în mai multe state membre poate demonstra conformitatea cu toate profilurile extinse relevante prin intermediul unui certificat european unic de securitate cibernetică.

(95) Obiectivele de securitate și cerințele de securitate prevăzute în sistemele europene de certificare a securității cibernetice în ceea ce privește securitatea produselor ar trebui să fie în concordanță cu cerințele esențiale de securitate cibernetică prevăzute în anexa I la Regulamentul (UE) 2024/2847. Această coerență este necesară pentru a se asigura că producătorii ale căror produse intră în domeniul de aplicare al Regulamentului (UE) 2024/2847 nu se confruntă cu cerințe contradictorii atunci când își certifică produsele în cadrul unui sistem european de certificare a securității cibernetice. În plus, coerența cerințelor facilitează prezumția de conformitate prevăzută la articolul 27 din Regulamentul (UE) 2024/2847, prin care producătorii de produse cu elemente digitale care au fost certificate în cadrul unui sistem european de certificare a securității cibernetice pot beneficia, în anumite condiții, de prezumția de conformitate cu cerințele esențiale de securitate cibernetică prevăzute în anexa I la regulamentul respectiv.

(96) În cadrul sistemului european de certificare a securității cibernetice, ar trebui să fie posibil să se specifice un profil de extindere, prin stabilirea unor cerințe suplimentare sau specifice pentru cazurile de utilizare, inclusiv capacități suplimentare, cum ar fi caracteristici îmbunătățite ale produselor, oferte sau active de servicii specializate, procese optimizate și măsuri de securitate avansate. Întrucât profilurile de extindere nu corespund unui nivel de asigurare specific, acestea ar trebui să descrie în detaliu scopul lor, inclusiv amenințările la adresa securității abordate. Profilurile de extindere sunt menite, în special, să demonstreze conformitatea cu standardele și cerințele de reglementare specifice, inclusiv, după caz, cu cerințele în ceea ce privește măsurile suplimentare de gestionare a riscurilor în materie de securitate cibernetică stabilite de un stat membru în conformitate cu principiul armonizării minime în conformitate cu Directiva (UE) 2022/2555.

(97) Fără a aduce atingere sistemului general de evaluare *inter pares* care urmează să fie instituit la nivelul tuturor autorităților naționale de certificare a securității cibernetice din cadrul ECCF, ar trebui să fie posibil să se includă în sistemele europene de certificare a securității cibernetice un mecanism de evaluare *inter pares* pentru organismele care eliberează certificate europene de securitate cibernetică pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate și postura de securitate cibernetică a entităților, în special pentru organismele care eliberează certificate cu un nivel de asigurare „ridicat” în cadrul acestor sisteme. Printre aceste organisme ar trebui să se numere și organismele de certificare ale autorităților naționale de certificare a securității cibernetice care eliberează certificate cu nivelul de asigurare „ridicat”. ECCG ar trebui să sprijine punerea în practică a acestor mecanisme de evaluare *inter pares*. Evaluările *inter pares* ar trebui să evalueze îndeosebi dacă organismele în cauză își îndeplinesc atribuțiile în mod armonizat și pot include mecanisme de recurs.

(98) Crizele precum războaiele, dezastrele naturale și pandemiile ar putea avea un impact negativ asupra activităților de certificare. În astfel de scenarii de criză, s-ar putea să nu fie fezabil, de exemplu, să se asigure securitatea site-ului din cauza distrugerii infrastructurii, a atacurilor cibernetice, a indisponibilității personalului și a inaccesibilității site-ului. Prin urmare, un sistem european de certificare a securității cibernetice ar trebui să specifice norme temporare privind continuitatea activităților de certificare în astfel de scenarii.

(99) Transpunerea propunerilor de sisteme tehnice în acte de punere în aplicare necesită cunoștințe tehnice și juridice complexe și poate crea o sarcină administrativă semnificativă. În plus, anumite elemente ale sistemelor europene de certificare a

securității cibernetice, cum ar fi gestionarea vulnerabilităților sau condițiile în care pot fi utilizate astfel de mărci sau etichete, sunt transsectoriale și pot beneficia de dispoziții de referință armonizate. Pentru a asigura calitatea sistemelor europene de certificare a securității cibernetice adoptate și pentru a reduce sarcina de asigurare a conformității pentru întreprinderi, Comisia ar trebui să fie împuternicită să adopte dispoziții-model care să acopere anumite elemente ale sistemelor europene de certificare a securității cibernetice.

(100) Pentru a asigura coerența cadrului european de certificare a securității cibernetice, ar trebui să fie posibil ca, în cadrul unui sistem european de certificare a securității cibernetice, să se specifice niveluri de asigurare pentru certificatele europene de securitate cibernetică și pentru declarațiile de conformitate UE eliberate în cadrul sistemului respectiv. Un certificat european de securitate cibernetică ar trebui să se refere la unul dintre nivelurile de asigurare: „de bază”, „substanțial” sau „ridicat”, în timp ce declarația de conformitate UE ar trebui să se refere numai la nivelul de asigurare „de bază”. Nivelurile de asigurare ar trebui să asigure rigoarea și profunzimea corespunzătoare evaluării produsului TIC, a serviciului TIC, a procesului TIC, a serviciului de securitate gestionat sau a posturii de securitate cibernetică a unei entități și ar trebui să fie caracterizate prin trimitere la specificațiile tehnice, la standardele și la procedurile aferente, inclusiv la controalele tehnice, al căror scop este de a atenua sau de a preveni incidentele. Fiecare nivel de asigurare ar trebui să fie coerent în cadrul diferitelor domenii sectoriale în care se aplică certificarea.

(101) Alegerea certificării adecvate și a cerințelor de securitate asociate de către utilizatorii certificatelor europene de securitate cibernetică ar trebui să se bazeze pe o analiză a riscurilor asociate utilizării produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate sau contextului de certificare a entităților. În consecință, nivelul de asigurare ar trebui să fie proporțional cu nivelul de risc asociat utilizării preconizate a produsului TIC, a serviciului TIC, a procesului TIC, a serviciilor de securitate gestionate sau cu mediul operațional și natura entității a cărei postură de securitate cibernetică face obiectul certificării.

(102) Pentru nivelul de asigurare „de bază”, evaluarea ar trebui să fie ghidată cel puțin de următoarele componente de asigurare: evaluarea ar trebui să includă cel puțin o examinare a documentației tehnice a produsului TIC, a serviciului TIC, a procesului TIC, a serviciului de securitate gestionat sau a posturii de securitate cibernetică a unei entități de către organismul de evaluare a conformității. În cazul în care certificarea include procese TIC, procesul utilizat pentru proiectarea, dezvoltarea și întreținerea unui produs TIC, a unui serviciu TIC, a unui serviciu de securitate gestionat sau a unei posturi de securitate cibernetică a unei entități ar trebui, de asemenea, să facă obiectul revizuirii tehnice. În cazul în care un sistem european de certificare a securității cibernetice prevede o autoevaluare a conformității, ar trebui să fie suficient ca producătorul sau furnizorul de produse TIC, e servicii TIC, de procese TIC sau de servicii de securitate gestionate sau entitatea a cărei postură de securitate cibernetică face obiectul certificării să fi efectuat o autoevaluare a conformității produsului TIC, a serviciului TIC, a procesului TIC, a serviciului de securitate gestionat sau a posturii de securitate cibernetică a unei entități cu sistemul de certificare.

(103) Pentru nivelul de asigurare „substanțial”, în plus față de elementele necesare pentru nivelul de asigurare „de bază”, evaluarea ar trebui să se bazeze cel puțin pe verificarea conformității funcționalităților de securitate ale produsului TIC, ale serviciului TIC, ale procesului TIC, ale serviciului de securitate gestionat sau ale posturii de securitate cibernetică a unei entități cu documentația sa tehnică.

(104) Pentru nivelul de asigurare „ridicat”, în plus față de elementele necesare pentru nivelul de asigurare „substanțial”, evaluarea ar trebui să se bazeze cel puțin pe un test de eficacitate care să evalueze rezistența funcțiilor de securitate împotriva atacurilor cibernetice elaborate lansate de persoane care au competențe și resurse semnificative. Activitățile de evaluare a conformității ar trebui să fie efectuate în Spațiul Economic European pentru nivelul de asigurare „ridicat” sau în cazul în care un sistem este conceput pentru a demonstra conformitatea și pentru a oferi prezumția de conformitate cu alte acte legislative ale Uniunii. Această cerință este justificată de faptul că activitățile de evaluare care au loc în afara Spațiului Economic European generează amenințări suplimentare la adresa securității cibernetice, în special proprietatea intelectuală a produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate sau a entităților evaluate. De exemplu, codul sursă al unui produs TIC ar putea fi examinat la trecerea frontierei unei țări terțe, ceea ce constituie un risc pentru proprietatea intelectuală. În plus, laboratoarele de testare stabilite în țări terțe nu își desfășoară activitatea într-un mediu vizat de măsurile de securitate cibernetică impuse de legislația UE, cum ar fi Directiva (UE) 2022/2555 sau Regulamentul (UE) 2024/2847. De exemplu, un laborator de testare se poate baza pe un furnizor terț de servicii cloud care nu respectă cerințele de securitate cibernetică prevăzute în Directiva (UE) 2022/2555. Cu toate acestea, ar trebui să se permită unui sistem de certificare să prevadă mecanisme de derogare, de exemplu în ceea ce privește certificarea site-urilor sau în alte cazuri în care activitățile de evaluare a conformității nu pot fi efectuate în mod rezonabil în Spațiul Economic European.

(105) În unele cazuri, ar putea fi necesare abordări diferite pentru îndeplinirea obiectivelor de securitate cu un anumit nivel de asigurare pentru a aborda particularitățile unui produs TIC, ale unui serviciu TIC, ale unui proces TIC, ale unor servicii de securitate gestionate sau ale unei posturi de securitate cibernetică a entităților. Pentru a permite o abordare mai detaliată, ar trebui să fie posibil ca, în cadrul unui sistem european de certificare a securității cibernetice, să se specifice unul sau mai multe niveluri de evaluare corespunzătoare unuia dintre nivelurile de asigurare. Acest lucru va permite dezvoltarea unor sisteme în care nivelurile multiple de evaluare concepute pentru un scop diferit vor corespunde nivelului de securitate asociat unui anumit nivel de asigurare.

(106) Sistemele europene de certificare a securității cibernetice ar trebui să prevadă posibilitatea efectuării unei evaluări a conformității pe răspunderea exclusivă a producătorului sau a furnizorului de produse TIC, de servicii TIC, de procese TIC sau de servicii de securitate gestionate sau a entității a cărei postură de securitate cibernetică este certificată („autoevaluare a conformității”). În aceste cazuri, ar trebui să fie suficient ca producătorul, furnizorul sau entitatea a cărei postură de securitate cibernetică este certificată să efectueze el (ea) însuși (însăși) toate verificările pentru a se asigura că produsele TIC, serviciile TIC, procesele TIC, serviciul de securitate gestionat sau postura de securitate cibernetică a unei entități este conformă cu sistemul european de certificare a securității cibernetice. Autoevaluarea conformității ar trebui să fie considerată adecvată pentru produsele TIC, serviciile TIC, procesele TIC, serviciul de securitate gestionat sau postura de securitate cibernetică a entității care au o complexitate scăzută, prezintă un risc scăzut pentru public și au o proiectare sau mecanisme de producție simple.

(107) În cazul în care un sistem european de certificare a securității cibernetice permite atât autoevaluări ale conformității, cât și certificări ale produselor TIC, ale serviciilor TIC, ale proceselor TIC, ale serviciilor de securitate gestionate sau ale posturii de securitate

cibernetică a entităților, într-un astfel de caz, sistemul de certificare ar trebui să prevadă mijloace clare și ușor de înțeles pentru consumatori sau alți utilizatori pentru a face distincție între produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura cibernetică a entităților autoevaluate și certificate de terți.

(108) Producătorul sau furnizorul de produse TIC, de servicii TIC, de procese TIC sau de servicii de securitate gestionate sau entitățile a căror postură de securitate cibernetică este certificată ar trebui să poată emite și semna declarația de conformitate UE ca parte a procedurii de evaluare a conformității. O declarație de conformitate UE este un document care prevede că un anumit produs TIC, serviciu TIC, proces TIC, serviciu de securitate gestionat sau postura de securitate cibernetică a unei entități respectă cerințele sistemului european de certificare a securității cibernetice. Prin emiterea și semnarea declarației de conformitate UE, producătorul sau furnizorul de produse TIC, de servicii TIC, de procese TIC sau de servicii de securitate gestionate sau entitatea a cărei postură de securitate cibernetică este certificată își asumă responsabilitatea pentru conformitatea produsului TIC, a serviciului TIC, a procesului TIC, a serviciului de securitate gestionat sau a posturii de securitate cibernetică a entității cu cerințele de securitate ale sistemului european de certificare a securității cibernetice. O copie a declarației de conformitate UE ar trebui transmisă autorității naționale de certificare a securității cibernetice și ENISA.

(109) Producătorii sau furnizorii de produse TIC, de servicii TIC, de procese TIC sau de servicii de securitate gestionate ori entitățile a căror postură de securitate cibernetică este certificată ar trebui să pună declarația de conformitate UE, documentația tehnică și toate celelalte informații relevante referitoare la conformitatea cu un sistem european de certificare a securității cibernetice la dispoziția autorității naționale de certificare a securității cibernetice competente pentru o perioadă prevăzută în sistemul european de certificare a securității cibernetice relevant și în conformitate cu legislația aplicabilă a Uniunii. Documentația tehnică ar trebui să specifice cerințele aplicabile în cadrul sistemului în măsura în care sunt relevante pentru autoevaluarea conformității. Documentația tehnică ar trebui compilată astfel încât să permită să se evalueze dacă un produs TIC, un serviciu TIC, un proces TIC sau un serviciu de securitate gestionat sau postura de securitate cibernetică a entității respectă cerințele aplicabile în cadrul sistemului.

(110) Certificatele europene de securitate cibernetică și declarațiile de conformitate UE ar trebui să îi ajute pe utilizatori să facă alegeri în cunoștință de cauză. Prin urmare, informațiile relevante ar trebui publicate pe un site administrat de ENISA. În plus, produsele TIC, serviciile TIC și procesele TIC care au fost certificate sau pentru care a fost emisă o declarație de conformitate UE ar trebui însoțite de informații structurate care sunt adaptate nivelului tehnic estimat al utilizatorului preconizat. Toți utilizatorii ar trebui să aibă acces la informații privind numărul de referință al sistemului de certificare, autoritatea sau organismul emitent și, după caz, nivelul de asigurare sau ar trebui să poată obține o copie a certificatului european de securitate cibernetică. Informațiile respective ar trebui să fie actualizate periodic și să fie disponibile pe un site dedicat privind sistemele europene de certificare a securității cibernetice. În plus, pentru a asigura accesibilitatea continuă, producătorii și furnizorii ar trebui să aibă obligația de a notifica organismul de certificare relevant în cazul în care se modifică locul în care se află informațiile online sau, după caz, informațiile fizice.

(111) O evaluare a conformității este o procedură prin care se evaluează dacă au fost îndeplinite cerințele specificate referitoare la un produs TIC, un serviciu TIC, un

proces TIC, un serviciu de securitate gestionat sau o entitate. Procedura respectivă este efectuată de o parte terță independentă care nu este producătorul sau furnizorul produselor TIC, al serviciilor TIC, al proceselor TIC sau al serviciilor de securitate gestionate care sunt certificate și nici entitatea a cărei postură de securitate cibernetică este evaluată. Ar trebui emis un certificat european de securitate cibernetică în urma evaluării reușite a unui produs TIC, a unui serviciu TIC, a unui proces TIC, a unui serviciu de securitate gestionat sau a unei posturi de securitate cibernetică a entității. Un certificat european de securitate cibernetică ar trebui să fie considerat drept o confirmare a faptului că evaluarea s-a derulat în mod adecvat.

(112) Separarea strictă a activităților de supraveghere și de certificare este importantă pentru a evita denaturările și interferențele care pot fi cauzate în situațiile în care entitatea care supraveghează piața concurează, de asemenea, pe aceeași piață. În consecință, activitățile în care autoritățile naționale de certificare a securității cibernetice doar își îndeplinesc rolul de supraveghere, de exemplu prin aprobarea prealabilă a eliberării unui certificat, nu ar trebui să necesite o separare internă suplimentară de alte activități de supraveghere. Aceasta include, de exemplu, o situație în care autoritatea națională de certificare a securității cibernetice colectează în mod activ informații pe parcursul procesului de certificare desfășurat de organismele private de evaluare a conformității și apoi își dă avizul cu privire la eliberarea certificatului de către organismele respective („modelul de aprobare prealabilă”).

(113) Sistemele europene de certificare a securității cibernetice ar trebui să specifice condițiile în care ar putea fi necesară recertificarea produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate sau a posturii de securitate cibernetică a unei entități sau în care ar putea fi necesară reducerea domeniului de aplicare al unui anumit certificat european de securitate cibernetică. În plus, sistemele europene de certificare a securității cibernetice ar trebui să țină seama de orice posibile efecte negative ale oricăror vulnerabilități sau neconformități detectate ulterior în ceea ce privește produsul TIC, serviciul TIC, procesul TIC, serviciul de securitate gestionat sau postura de securitate cibernetică certificat(ă) a unei entități în ceea ce privește conformitatea cu cerințele de securitate ale certificatului respectiv.

(114) Armonizarea joacă un rol esențial în asigurarea unei securități cibernetice solide și în îmbunătățirea accesului pe piață pentru întreprinderi. În schimb, fragmentarea și lipsa recunoașterii reciproce a certificatelor reprezintă obstacole semnificative în calea fluxului neîntrerupt de date, sporind astfel costurile operaționale pentru industria Uniunii. Pentru a atenua aceste provocări, este esențial să se evite fragmentarea atât a domeniului de aplicare al controalelor de securitate, cât și a metodelor de evaluare a conformității în întreaga Uniune.

(115) Statele membre ar trebui să informeze Comisia și ECCG cu suficient timp în prealabil înainte de adoptarea unor noi sisteme naționale de certificare a securității cibernetice pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura de securitate cibernetică a entităților, pentru a ajuta Comisia și ECCG să evalueze impactul noului sistem național de certificare a securității cibernetice asupra bunei funcționări a pieței interne și având în vedere orice interes strategic de a solicita un sistem european de certificare a securității cibernetice.

(116) Trimiterile din legislația națională la standarde naționale care au încetat să mai producă efecte ca urmare a intrării în vigoare a unui sistem european de certificare a securității cibernetice poate constitui o sursă de confuzie. Prin urmare, după caz,

statele membre ar trebui să reflecte adoptarea unui sistem european de certificare a securității cibernetice în legislația lor națională.

(117) Pentru a facilita dezvoltarea unei piețe interne fiabile, creând în același timp parteneriate cu țări terțe, procesul de certificare instituit în cadrul ECCF ar trebui pus în aplicare într-un mod care să faciliteze recunoașterea internațională, recunoașterea reciprocă și alinierea la standardele internaționale.

(118) Pentru a facilita și mai mult comerțul și recunoscând că lanțurile de aprovizionare TIC sunt internaționale, Uniunea poate încheia acorduri de recunoaștere reciprocă privind certificatele europene de securitate cibernetică, în conformitate cu articolul 218 din TFUE. Comisia ar trebui să fie împuternicită să adopte acte de punere în aplicare pentru a recunoaște în mod unilateral echivalența certificatelor țărilor terțe cu certificatele europene de securitate cibernetică. Ar trebui să fie posibil să se prevadă condiții specifice pentru o astfel de recunoaștere a certificatelor țărilor terțe.

(119) Pentru a realiza punerea în aplicare echivalentă a cadrului pe întreg teritoriul Uniunii, a facilita recunoașterea reciprocă și a promova acceptarea generală a certificatelor europene de securitate cibernetică și a declarațiilor de conformitate UE, este necesar să se instituie un sistem de evaluare *inter pares* în rândul autorităților naționale de certificare a securității cibernetice. Evaluarea *inter pares* ar trebui să vizeze procedurile de supraveghere a conformității produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate și a posturii de securitate cibernetică a entităților cu certificatele europene de securitate cibernetică, procedurile de monitorizare a obligațiilor producătorilor sau furnizorilor de produse TIC, de servicii TIC, de procese TIC, de servicii de securitate gestionate și ale entităților certificate care efectuează autoevaluarea conformității, procedurile de monitorizare a organismelor de evaluare a conformității, precum și caracterul adecvat al expertizei personalului organismelor care eliberează certificate pentru nivelul de asigurare „ridicat”. ENISA ar trebui să participe la evaluările *inter pares* în calitate de observator și să sprijine organizarea mecanismului de evaluare *inter pares* și a evaluărilor *inter pares*, inclusiv prin elaborarea de documente de orientare și modele relevante, în cooperare cu Comisia și cu ECCG. ENISA ar trebui, de asemenea, să pună la dispoziția publicului, pe site-ul său privind sistemele europene de certificare a securității cibernetice, informațiile privind calendarul evaluărilor *inter pares* și lista autorităților naționale de certificare a securității cibernetice evaluate *inter pares* care urmează să ducă la îndeplinire calendarul. Regulamentul de punere în aplicare (UE) 2025/2540 al Comisiei[60], adoptat în temeiul Regulamentului (UE) 2019/881, stabilește planul pentru evaluările *inter pares* care este utilizat de sistemele europene de certificare a securității cibernetice adoptate. Este necesar să se asigure continuarea evaluărilor *inter pares*. Cu toate acestea, Comisia ar trebui să fie în măsură, prin intermediul unor acte de punere în aplicare, dacă este necesar, să stabilească un nou plan pentru evaluările *inter pares* de cel puțin cinci ani, precum și să stabilească criterii și metodologii pentru funcționarea sistemului de evaluare *inter pares*.

(120) După adoptarea unui sistem european de certificare a securității cibernetice, producătorii sau furnizorii de produse TIC, de servicii TIC, de procese TIC, de servicii

[60] Regulamentul de punere în aplicare (UE) 2025/2540 al Comisiei din 9 decembrie 2025 de stabilire a normelor de aplicare a Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului în ceea ce privește stabilirea planului de evaluare *inter pares* (JO L 2540, 12.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/2540/oj).

de securitate gestionate sau entitățile a căror postură de securitate cibernetică face obiectul certificării ar trebui să poată depune cereri de certificare a produselor lor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate sau a posturii de securitate cibernetică la organismul de evaluare a conformității ales de ei oriunde în Uniune. Organismele de evaluare a conformității ar trebui să fie acreditate de un organism național de acreditare dacă îndeplinesc cerințele prevăzute în prezentul regulament și, după caz, cerințele specificate de Comisie în conformitate cu prezentul regulament. Sistemul stabilit în prezentul regulament ar trebui completat de sistemul de acreditare prevăzut în Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului[61].

(121) Organismele de evaluare a conformității care au fost acreditate sau notificate în temeiul legislației existente a Uniunii, în special al Regulamentului (UE) 2024/2847 sau al Regulamentului de punere în aplicare (UE) 2024/482, ar putea deține competențe relevante pentru sistemele europene de certificare a securității cibernetice nou adoptate. Pentru a evita sarcinile financiare și administrative inutile, este oportun să se creeze sinergii pentru acreditarea organismelor de evaluare a conformității în temeiul prezentului regulament. Din acest motiv, cerințele de acreditare ale sistemelor ar trebui stabilite astfel încât să existe o aliniere cât mai mare posibil la cerințele referitoare la organismele notificate prevăzute în Regulamentul (UE) 2024/2847 și la cerințele de acreditare prevăzute în Regulamentul de punere în aplicare (UE) 2024/482. În plus, organismele de evaluare a conformității care sunt supuse unui proces de acreditare în temeiul prezentului regulament ar trebui să se poată baza pe rezultatele anterioare ale evaluării competențelor lor în temeiul altor acte legislative ale Uniunii, ori de câte ori există o suprapunere a cerințelor de acreditare.

(122) Pentru a facilita servicii armonizate de evaluare a conformității în întreaga Uniune, ar trebui să fie posibil să se stabilească într-un sistem european de certificare a securității cibernetice cerințe suplimentare sau specifice pentru organismele de evaluare a conformității. În contextul certificării, o autorizație ar trebui înțeleasă ca o decizie a unei autorități naționale de certificare a securității cibernetice conform căreia un organism de evaluare a conformității îndeplinește cerințele specifice sau suplimentare prevăzute într-un sistem european de certificare a securității cibernetice, pentru a desfășura o activitate specifică de evaluare a conformității.

(123) În cazul în care un sistem european de certificare a securității securitate cibernetice stabilește cerințe suplimentare sau specifice în conformitate cu prezentul regulament, organismele de evaluare a conformității ar trebui să fie autorizate de autoritățile naționale de certificare a securității cibernetice să îndeplinească sarcini în cadrul unui astfel de sistem. Pentru a evita autorizarea multiplă, pentru a îmbunătăți acceptarea și recunoașterea deciziilor de autorizare și pentru a efectua o monitorizare eficace a organismelor autorizate de evaluare a conformității, organismele de evaluare a conformității ar trebui să solicite autorizarea de către autoritatea națională de certificare a securității cibernetice a statului membru în care sunt stabilite. Cu toate acestea, este necesar să se asigure că un organism de evaluare a conformității poate solicita autorizarea într-un alt stat membru în cazul în care nu există o autoritate națională de certificare a securității cibernetice în propriul stat membru sau în cazul în

[61] Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/93 (JO L 218, 13.8.2008, p. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

care autoritatea națională de certificare a securității cibernetice nu are competența de a furniza serviciile de autorizare solicitate. În astfel de cazuri, ar trebui să se asigure o cooperare și un schimb de informații adecvate între autoritățile naționale de certificare a securității cibernetice. Comisia ar trebui să fie împuternicită să adopte acte de punere în aplicare de stabilire a procedurilor de autorizare, inclusiv pentru cooperarea transfrontalieră în ceea ce privește autorizarea.

(124) Pentru a garanta nivelul de protecție necesar pentru un produs TIC, un serviciu TIC, un proces TIC, un serviciu de securitate gestionat sau o postură de securitate cibernetică a unei entități, este esențial ca subcontractanții și filialele de evaluare a conformității să aibă obligația de a îndeplini aceleași cerințe ca organismele notificate de evaluare a conformității în ceea ce privește îndeplinirea sarcinilor de evaluare a conformității. În consecință, un organism de evaluare a conformității ar trebui să aibă competența corespunzătoare și să fie în măsură să verifice dacă cerințele aplicabile sunt îndeplinite de subcontractanții săi.

(125) Măsura în care organismul de evaluare a conformității intenționează să se bazeze pe subcontractanți stabiliți în afara Uniunii sau care au acces la personal sau instalații din afara statului membru de notificare ar trebui să fie evaluată în mod corespunzător de către autoritatea de notificare. Autoritatea publică a unui stat membru ar trebui să aibă posibilitatea de a decide că nu își poate asuma responsabilitatea generală în calitate de autoritate națională de certificare a securității cibernetice pentru un astfel de acord și de a retrage sau limita domeniul de aplicare al notificării.

(126) Pentru a evalua cerințele de securitate cibernetică pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura de securitate cibernetică a entităților, autoritățile naționale de certificare a securității cibernetice ar trebui să notifice Comisiei și celorlalte state membre organismele acreditate de evaluare a conformității. Notificarea organismelor de evaluare a conformității acreditate și, după caz, autorizate indică faptul că organismele respective pot fi de încredere în desfășurarea activităților de evaluare și certificare în conformitate cu prezentul regulament și cu sistemul european de certificare a securității cibernetice, contribuind la reputația generală a certificării europene de securitate cibernetică. Prin urmare, este esențial să se asigure că organismele de evaluare a conformității care au fost notificate îndeplinesc cerințele și obligațiile care le revin în timp și că lista organismelor notificate de evaluare a conformității este actualizată.

(127) Regulamentul de punere în aplicare (UE) 2024/3143 al Comisiei[62], adoptat în temeiul Regulamentului (UE) 2019/881, stabilește circumstanțele, formatele și procedurile pentru notificările organismelor de evaluare a conformității care sunt utilizate de sistemele europene de certificare a securității cibernetice adoptate. Prin urmare, este necesar să se asigure continuarea activităților de notificare. Cu toate acestea, Comisia ar trebui să fie împuternicită să adopte acte de punere în aplicare pentru a adapta circumstanțele, procedurile și formatele respective pentru notificarea organismelor de evaluare a conformității. În acest context, Comisia ar trebui să se bazeze pe experiența dobândită în contextul sistemelor existente și să urmărească alinierea la alte acte

[62] Regulamentul de punere în aplicare (UE) 2024/3143 al Comisiei din 18 decembrie 2024 de stabilire a circumstanțelor, a formatelor și a procedurilor pentru notificările efectuate în temeiul articolului 61 alineatul (5) din Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor (JO L 3143, 19.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

legislative și cadre relevante ale Uniunii, în special la Regulamentul (UE) 2024/2847 și la noul cadru legislativ, în vederea reducerii sarcinii de asigurare a conformității pentru organismele de evaluare a conformității care își desfășoară activitatea în temeiul diferitelor instrumente juridice.

(128) Lanțurile de aprovizionare din domeniul tehnologiei informației și comunicațiilor (TIC) sunt compuse dintr-un set corelat de resurse și procese între operatorii economici. Lanțurile de aprovizionare TIC joacă un rol esențial în susținerea stabilității societății și în stimularea activității economice în întreaga Uniune. Acestea joacă, de asemenea, un rol esențial în facilitarea infrastructurii digitale în Uniune și sprijină funcționarea societății și a economiei Uniunii. Lanțurile de aprovizionare TIC permit fabricarea, producția, distribuția și întreținerea serviciilor TIC, a sistemelor TIC și a produselor TIC care stau la baza diferitelor sectoare critice și extrem de critice, inclusiv asistența medicală, finanțele, transporturile, telecomunicațiile, energia și vămile. Securitatea lanțurilor de aprovizionare TIC ale acestor sectoare critice poate avea, de asemenea, un impact asupra securității infrastructurii militare și de apărare, în cazul în care această infrastructură se bazează pe sectoare critice civile și pe lanțurile lor de aprovizionare TIC. Cu toate acestea, potrivit raportului privind situația amenințărilor la adresa securității cibernetice publicat de ENISA (*ENISA Threat Landscape 2025*)[63], atacurile la nivelul lanțurilor de aprovizionare se numără printre cele cinci amenințări principale la adresa securității cibernetice, care arată că atacatorii mobilizează în mod activ căi indirecte prin intermediul furnizorilor terți și al dependențelor. Perturbarea lanțurilor de aprovizionare TIC poate împiedica desfășurarea activităților economice pe piața internă, poate genera pierderi financiare, poate submina încrederea utilizatorilor și poate provoca pagube majore economiei și societății Uniunii. Prin urmare, pregătirea și eficacitatea în materie de securitate cibernetică sunt mai importante ca niciodată pentru buna funcționare a pieței interne.

(129) Pe lângă riscurile tehnice care sunt abordate de Directiva (UE) 2022/55 a Parlamentului European și a Consiliului[64], de Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului[65] și de cadrul european de certificare a securității cibernetice instituit prin Regulamentul (UE) 2019/881, lanțurile de aprovizionare TIC sunt din ce în ce mai expuse unor riscuri non-tehnice. Astfel de riscuri non-tehnice pot fi legate de jurisdicția căreia îi este supus un furnizor de anumite componente, în special în cazul în care o țară terță sau actori care generează amenințări controlați din țara respectivă se implică în spionaj economic, desfășoară activități sau campanii cibernetice răuvoitoare împotriva Uniunii sau a statelor sale membre sau adoptă un comportament statal iresponsabil în spațiul cibernetic, dar nu se limitează la aceasta. riscurile non-tehnice pot fi, de asemenea, legate de vulnerabilități ascunse sau de uși secrete sau de potențiale perturbări sistemice ale aprovizionării, în special în cazul blocajului tehnologic sau al dependenței de furnizori. De exemplu,

---

63 *ENISA Threat Landscape 2025* (Raportul privind situația amenințărilor pentru 2025), octombrie 2025.

64 Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (JO L 333, 27.12.2022, p. 80, ELI: https://eur-lex.europa.eu/eli/dir/2022/2555/oj).

65 Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentelor (UE) nr. 168/2013 și (UE) 2019/1020, precum și a Directivei (UE) 2020/1828 (Regulamentul privind reziliența cibernetică) (JO L, 2024/2847, 20.11.2024, ELI: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng).

comutatoarele de eliminare ar putea fi utilizate pentru a afecta disponibilitatea rețelelor de comunicații și a rețelelor de energie electrică.

(130) Comunicarea comună privind consolidarea securității economice a UE[66] a subliniat riscul ca țările terțe să obțină acces la informații și date sensibile în Uniune sau în statele sale membre, fie ca urmare a spionajului industrial, a furnizării de hardware sau software utilizat în anumite produse, fie ca urmare a dreptului lor de proprietate și a controlului asupra anumitor întreprinderi care dețin informații și date sensibile. Aceasta a subliniat, de asemenea, riscul ca infrastructura critică a Uniunii – inclusiv transportul critic, sistemele spațiale, infrastructura energetică și de comunicații, în special cele care sunt identificate ca fiind strategice pentru mobilitatea militară – să fie perturbată de actori străini, ceea ce ar putea duce la efecte în cascadă asupra economiei Uniunii. Perturbările ar putea apărea prin atacuri fizice, cibernetice sau hibride, inclusiv sabotajul unor întregi instalații sau al unor părți sau subcomponente ale acestora. Acestea ar putea fi, de asemenea, legate de lanțurile de aprovizionare TIC, pe care se bazează componentele sau serviciile critice pentru infrastructurile esențiale.

(131) Ca răspuns la provocările la adresa securității lanțului de aprovizionare TIC generate de riscurile non-tehnice, unele state membre au luat măsuri de reglementare, inclusiv desemnarea furnizorilor cu grad ridicat de risc, fiind probabil ca alte state membre să facă acest lucru. Acest lucru ar putea duce la noi divergențe între abordările naționale și, în cele din urmă, la o vulnerabilitate mai mare a unor state membre, cu potențiale efecte de propagare în întreaga Uniune. Prin urmare, este necesar să se armonizeze anumite aspecte legate de riscurile non-tehnice în materie de securitate cibernetică la nivelul lanțurilor de aprovizionare TIC. O astfel de intervenție la nivelul Uniunii este, de asemenea, justificată având în vedere necesitatea de a asigura un nivel ridicat de securitate cibernetică în întreaga Uniune. Dispozițiile privind securitatea lanțului de aprovizionare TIC vizează eliminarea unor divergențe mari între statele membre, în special prin stabilirea unor norme pentru mecanismele de evaluare a riscurilor legate de securitatea lanțului de aprovizionare TIC la nivelul Uniunii și a unor standarde minime de protecție împotriva riscurilor lanțului de aprovizionare TIC.

(132) Pentru a reduce dependențele și vulnerabilitățile critice, este necesar să se instituie un cadru fiabil în ceea ce privește lanțurile de aprovizionare TIC, care ar trebui să abordeze riscurile non-tehnice legate de furnizorii cu grad ridicat de risc și dependențele din sectoarele cu o importanță critică ridicată și din alte sectoare critice. Prin urmare, este necesar să se prevadă un cadru obiectiv, bazat pe riscuri, adaptat exigențelor viitorului și neutru din punct de vedere tehnologic la nivelul Uniunii, să se identifice activele TIC esențiale și să se prevadă un set de măsuri de atenuare proporționale pentru a aborda riscurile.

(133) Riscurile în materie de securitate cibernetică, inclusiv riscurile legate de dependența de furnizori cu grad ridicat de risc, pot fi observate în mai multe lanțuri de aprovizionare TIC critice din Uniune, inclusiv în ceea ce privește echipamentele de detectare, vehiculele conectate și automatizate, sistemele de alimentare cu energie electrică și stocarea energiei electrice, sistemele de alimentare cu apă, dronele și sistemele anti-drone, serviciile de cloud computing, dispozitivele medicale, echipamentele de supraveghere, serviciile spațiale și semiconductorii. De exemplu, vulnerabilitățile echipamentelor de detectare a securității ar putea acorda acces la sistemele TIC,

[66] Comunicare comună către Parlamentul European și Consiliu, Consolidarea securității economice a UE, 3 decembrie 2025, JOIN(2025) 977 final.

permițând actorilor răuvoitori să manipuleze scanerele astfel încât articole interzise să poată fi introduse prin punctul de control de securitate fără a fi detectate, cu posibile consecințe catastrofale.

(134) Prezentul regulament nu ar trebui să împiedice statele membre să adopte sau să mențină dispoziții care să asigure un nivel mai ridicat de securitate cibernetică în ceea ce privește securitatea lanțului de aprovizionare TIC, cu condiția ca aceste dispoziții să fie în concordanță cu obligațiile statelor membre prevăzute în dreptul Uniunii. Astfel de dispoziții pot include, de exemplu, impunerea unor măsuri de atenuare mai stricte în ceea ce privește activele TIC esențiale.

(135) Pentru a identifica riscurile potențiale în materie de securitate cibernetică care afectează anumite lanțuri de aprovizionare TIC, grupul de cooperare instituit prin articolul 14 din Directiva (UE) 2022/2555 („Grupul de cooperare NIS”) poate evalua lanțuri de aprovizionare TIC specifice prin intermediul unor evaluări coordonate la nivelul Uniunii ale riscurilor în materie de securitate. Evaluările coordonate la nivelul Uniunii ale riscurilor în materie de securitate ar trebui să analizeze, printre altele, principalii actori care generează amenințări, principalele amenințări și vulnerabilități care afectează activele TIC esențiale. Evaluările coordonate la nivelul Uniunii ale riscurilor în materie de securitate ar trebui să elaboreze o listă de scenarii de risc și o listă de măsuri de atenuare a riscurilor. Evaluările coordonate la nivelul Uniunii ale riscurilor în materie de securitate ar trebui finalizate în termen de șase luni. În caz de urgență specifică, ar trebui să fie posibilă scurtarea termenelor.

(136) În cazurile în care Comisia are motive suficiente să considere că există o amenințare cibernetică semnificativă pentru securitatea Uniunii legată de lanțurile de aprovizionare TIC critice și că ar putea fi necesară o acțiune pentru a menține buna funcționare a pieței interne, aceasta ar trebui să consulte fără întârziere statele membre cu privire la necesitatea unor măsuri de atenuare și să efectueze o evaluare a riscurilor în materie de securitate, ținând seama de consultarea statelor membre.

(137) În cazul în care, în urma unei evaluări a riscurilor în materie de securitate efectuate de grupul de cooperare NIS sau de Comisie, reiese că o anumită țară terță prezintă riscuri grave și structurale non-tehnice în materie de securitate cibernetică pentru lanțurile de aprovizionare TIC, Comisia ar trebui să verifice amenințarea reprezentată de țara respectivă. Comisia poate iniția o astfel de verificare și pe baza altor surse, cum ar fi o declarație publică în numele Uniunii sau al unui stat membru ca răspuns la cazurile de comportament iresponsabil al statelor în spațiul cibernetic care au condus la un incident de securitate cibernetică. Pentru a evalua nivelul de amenințare, Comisia ar trebui să țină seama de elemente precum existența în țara terță a unor legi sau practici care impun entităților aflate sub jurisdicția lor să raporteze autorităților din țara terță respectivă informații privind vulnerabilitățile software sau hardware înainte să se fi știut că vulnerabilitățile respective a fost exploatate. Un alt element relevant este absența unor căi de atac judiciare eficace și a unor mecanisme de control independente și democratice care să poată corecta preocupările în materie de securitate, inclusiv cu privire la practicile existente, informațiile fundamentate cu privire la incidentele unor actori care generează amenințări care își desfășoară activitatea în afara teritoriului țării respective și care desfășoară activități sau campanii cibernetice răuvoitoare, precum și lipsa capacității sau a voinței țării terțe de a coopera cu Comisia sau cu statele membre pentru a aborda riscul care decurge din funcționarea unor astfel de actori care generează amenințări. Comisia ar trebui, de asemenea, să țină seama de informațiile care decurg din evaluările coordonate la nivelul Uniunii ale riscurilor în materie de

securitate sau din rapoartele emise de statele membre sau de organizații internaționale, cum ar fi NATO.

(138) În sensul prezentului regulament, noțiunea de control ar trebui înțeleasă ca fiind capacitatea de a exercita o influență decisivă asupra unei entități juridice în mod direct sau indirect, prin intermediul uneia sau mai multor entități juridice intermediare. Controlul entităților dintr-o țară terță care prezintă motive de îngrijorare în materie de securitate cibernetică ar trebui, de asemenea, să fie stabilit în situațiile în care o astfel de entitate are structuri de conducere executivă în țara respectivă.

(139) Uniunea nu ar trebui să finanțeze proiecte care implică furnizori cu grad ridicat de risc, care ar pune în pericol securitatea Uniunii și ar submina interesele și credibilitatea Uniunii. Furnizorii cu grad ridicat de risc identificați în temeiul prezentului regulament nu ar trebui, prin urmare, să aibă dreptul de a participa la niciun program și instrument de finanțare al Uniunii pus în aplicare în cadrul gestiunii directe și indirecte în conformitate cu articolul 136 din Regulamentul (UE/Euratom) 2024/2509 și cu normele sectoriale specifice ale Uniunii, precum și la nicio activitate de finanțare a Uniunii pusă în aplicare în cadrul gestiunii partajate, inclusiv în următorul cadru financiar multianual în ceea ce privește furnizarea de componente TIC sau de componente care includ componente TIC ce urmează să fie utilizate în activele TIC esențiale identificate. Partenerii de implementare ai Uniunii, cum ar fi Grupul Băncii Europene de Investiții și băncile și instituțiile naționale de promovare, ar trebui să se abțină de la sprijinirea proiectelor care contravin celor de mai sus, inclusiv în cadrul operațiunilor pe risc propriu.

(140) Achizițiile publice pot fi un instrument puternic pentru ca autoritățile publice să contribuie la o economie mai inovatoare, mai durabilă și mai competitivă și pentru cheltuirea fondurilor publice într-un mod strategic. Achizițiile publice legate de lanțurile de aprovizionare TIC nu ar trebui utilizate în beneficiul furnizorilor care amenință securitatea infrastructurii critice a Uniunii. Furnizorii cu grad ridicat de risc identificați în temeiul prezentului regulament nu ar trebui, prin urmare, să aibă dreptul de a participa la achizițiile publice privind furnizarea de componente TIC sau de componente care includ componente TIC care urmează să fie utilizate în activele TIC esențiale identificate.

(141) Certificarea securității cibernetice joacă un rol în consolidarea securității generale și în combaterea amenințărilor cibernetice, servind drept criteriu de referință pentru încredere. Această încredere ar putea fi erodată dacă atestatele de competențe în materie de securitate cibernetică ar fi eliberate de furnizori cu grad ridicat de risc care, prin urmare, nu ar trebui să aibă dreptul de a solicita să devină furnizori autorizați ai niciunui atestat individual de competențe în materie de securitate cibernetică al Uniunii. În mod similar, este, de asemenea, oportun să se excludă furnizorii cu grad ridicat de risc de la obținerea certificării de securitate cibernetică în temeiul ECCF și de la a deveni organisme acreditate de evaluare a conformității care să elibereze astfel de certificate.

(142) Standardele de securitate cibernetică joacă un rol esențial în securitatea și fiabilitatea infrastructurilor digitale. Este necesar să se ia măsuri adecvate pentru a asigura standardizarea în domeniul securității cibernetice. Implicarea entităților stabilite sau controlate din țări care au fost identificate ca prezentând motive de îngrijorare în materie de securitate cibernetică pentru lanțul de aprovizionare TIC în conformitate cu prezentul regulament poate conduce la influențarea standardelor de securitate cibernetică într-un mod care le subminează securitatea și credibilitatea.

(143) Pe baza rezultatelor evaluărilor riscurilor în materie de securitate, Comisia poate identifica, prin intermediul unor acte de punere în aplicare, activele TIC care ar trebui considerate active TIC esențiale din cauza caracterului lor critic și sub rezerva unor măsuri specifice de atenuare. Simpla existență a posibilității de conectivitate a activului ar trebui să fie suficientă pentru a lua în considerare riscul său în materie de securitate cibernetică.

(144) În cazul în care este necesar pentru a asigura un nivel ridicat de securitate cibernetică, reziliență cibernetică și încredere în Uniune, măsurile de atenuare pot fi aplicate entităților în ceea ce privește lanțul lor de aprovizionare TIC și, în special, activele TIC esențiale identificate. Măsurile de atenuare propuse ar trebui să se bazeze pe evaluarea riscurilor și a dependențelor potențiale, inclusiv a impactului economic și societal potențial al unor astfel de măsuri asupra entităților în cauză care își desfășoară activitatea în sectoare extrem de critice sau în alte sectoare critice, în special asupra IMM-urilor. Evaluarea impactului economic ar trebui să analizeze costurile punerii în aplicare a măsurilor de atenuare, inclusiv durata ciclului de viață al componentelor relevante din activele TIC esențiale, în cazul în care măsurile includ înlocuirea furnizorilor. Disponibilitatea unor furnizori alternativi pe piață ar trebui, de asemenea, evaluată pentru a asigura furnizarea continuă a serviciilor.

(145) Întrucât măsurile de atenuare ar putea avea un efect restrictiv asupra comerțului internațional cu bunuri și servicii, acestea ar trebui să fie proporționale și specifice pentru a urmări obiectivul legitim de a asigura securitatea cibernetică a lanțurilor de aprovizionare TIC în ceea ce privește entitățile de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555, în conformitate cu obligațiile internaționale ale Uniunii.

(146) Utilizarea, instalarea sau orice alt tip de integrare a componentelor furnizate de furnizorii cu grad ridicat de risc în exploatarea activelor TIC esențiale poate fi legată de riscurile transferurilor ulterioare de date către o țară terță. În special, riscurile pot fi reprezentate de un nivel insuficient de protecție a datelor în țara terță, cum ar fi pentru protecția drepturilor fundamentale, a proprietății intelectuale sau a secretelor comerciale, sau de accesul și exploatarea ilegale ale datelor respective în vederea unor posibile perturbări viitoare ale lanțului de aprovizionare și în scopuri de spionaj. Pentru a atenua astfel de riscuri, se pot aplica restricții în ceea ce privește transferul anumitor tipuri de date către țări terțe.

(147) Vulnerabilitățile importante decurg din lipsa diversității echipamentelor utilizate de entitățile de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555. Dependența de un singur furnizor creează o dependență de anumite echipamente sau soluții. Lipsa diversității furnizorilor sporește vulnerabilitatea generală a infrastructurii critice, în special dacă entitățile se aprovizionează cu componentele lor TIC utilizate în active TIC sensibile de la un furnizor care prezintă un grad ridicat de risc. Dependența afectează, de asemenea, în mod semnificativ reziliența la nivel național și la nivelul Uniunii și creează puncte unice de defecțiune. Pentru a atenua aceste riscuri, se pot aplica cerințe de a avea mai mulți furnizori pentru anumite active TIC esențiale.

(148) Entitățile Uniunii pot utiliza, de asemenea, active esențiale, astfel cum sunt definite în prezentul regulament. Prin urmare, normele prevăzute în prezentul regulament privind securitatea lanțului de aprovizionare TIC ar trebui să li se aplice și acestora. Pentru a se asigura că se ține seama de specificitatea entităților Uniunii, este important să se ia în considerare riscurile non-tehnice de la nivelul lanțurilor de aprovizionare TIC în

ceea ce privește entitățile Uniunii atunci când se efectuează evaluări coordonate la nivelul Uniunii ale riscurilor de securitate.

(149) În circumstanțe excepționale care justifică o intervenție imediată pentru a menține buna funcționare a pieței interne și în cazul în care există dovezi clare care oferă Comisiei motive suficiente pentru a considera că utilizarea componentelor TIC sau a componentelor care includ componente TIC de la un anumit furnizor reprezintă o amenințare semnificativă la adresa securității cibernetice pentru activitățile economice sau societale ale cel puțin trei state membre, Comisia poate propune, în strânsă consultare cu statele membre, interzicerea utilizării, a instalării sau a integrării unor astfel de componente de la acest furnizor în funcție de tipul de entități menționate în anexele I și II la Directiva (UE) 2022/2555.

(150) Pentru a asigura proporționalitatea măsurilor aplicate, entitățile stabilite într-o țară terță care prezintă motive de îngrijorare în materie de securitate cibernetică, desemnate în conformitate cu prezentul regulament sau controlate de o astfel de țară terță, de către o entitate stabilită într-o astfel de țară terță sau de către un resortisant al unei astfel de țări terțe pot solicita să fie exceptate de la interdicția de a furniza entităților de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555 componente TIC sau componente care includ componente TIC pentru utilizarea, instalarea sau integrarea lor în activele TIC esențiale ale entității respective și de a participa la procedurile de achiziții publice organizate în conformitate cu legislația de transpunere a Directivelor 2014/24/UE[67] și 2014/25/UE ale Parlamentului European și ale Consiliului[68] în ceea ce privește furnizarea de componente TIC sau componente care includ componente TIC ce urmează să fie utilizate în activele TIC esențiale identificate. În acest scop, entitatea ar trebui să demonstreze cu dovezi clare că aplică măsuri eficace de abordare a riscurilor non-tehnice și de asigurare a absenței oricărei posibile interferențe nejustificate din partea unei țări terțe care ridică probleme de securitate cibernetică.

(151) Rețelele de comunicații electronice constituie coloana vertebrală a unei game largi de servicii care sunt esențiale pentru funcționarea pieței interne și pentru menținerea și funcționarea funcțiilor societale și economice vitale – cum ar fi energia, transporturile, serviciile bancare, sănătatea, apărarea, precum și sistemele de control industrial. Prin urmare, aceste rețele extrem de critice sunt ținte atractive pentru toate tipurile de atacuri cibernetice și amenințări hibride, pentru perturbări, spionaj, colectarea de informații, precum și pentru fraudă și infracțiuni financiare. Evaluarea riscurilor efectuată de Grupul de cooperare NIS privind securitatea cibernetică și reziliența infrastructurilor și rețelelor de comunicații din Europa a identificat o serie de riscuri și amenințări de importanță strategică din perspectiva Uniunii, cum ar fi atacurile de tip wiper/ransomware, atacurile asupra lanțului de aprovizionare, intruziunile în rețea și atacurile de tip DDoS (*Distributed denial-of-service*).

(152) Având în vedere interconectarea și interdependența dintre diferitele rețele naționale de comunicații electronice, este necesar ca toate statele membre să ia măsurile

---

67 Directiva 2014/24/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile publice și de abrogare a Directivei 2004/18/CE (JO L 94, 28.3.2014, p. 65, ELI: https://eur-lex.europa.eu/eli/dir/2014/24/oj/eng).

68 Directiva 2014/25/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile efectuate de entitățile care își desfășoară activitatea în sectoarele apei, energiei, transporturilor și serviciilor poștale și de abrogare a Directivei 2004/17/CE (JO L 94, 28.3.2014, p. 243, ELI: https://eur-lex.europa.eu/eli/dir/2014/25/oj?locale=fr).

corespunzătoare pentru a asigura securitatea rețelelor lor. Din aceleași motive, este necesar să existe un cadru juridic eficace la nivelul Uniunii care să abordeze și riscurile non-tehnice și să asigure securitatea rețelelor de comunicații electronice interconectate într-un mod cuprinzător.

(153) În special, securitatea cibernetică a rețelelor 5G este o chestiune de importanță strategică pentru Uniune, deoarece aceste rețele constituie coloana vertebrală a unei game largi de servicii de importanță esențială pentru funcționarea pieței interne și sunt, de asemenea, esențiale pentru asigurarea pregătirii noastre pentru apărare, inclusiv în ceea ce privește mobilitatea militară. Rețelele 5G sunt capabile să asigure o conectivitate ultrarapidă fiabilă, de exemplu pentru schimbul de date și informații, detectarea dronelor și coordonarea în timp real a câmpurilor de luptă.

(154) Implementarea tehnologiei 5G constă în principal în rețele neautonome, în care numai rețeaua de acces radio este modernizată la tehnologia 5G, în timp ce restul rețelei se bazează în continuare pe o rețea nucleu 4G existentă. Rețelele 5G neautonome se bazează în principal pe infrastructura deja existentă, ceea ce înseamnă că securitatea viitoarelor rețele 5G este determinată, într-o anumită măsură, de echipamentele de rețea deja existente și de configurația acestor echipamente. Prin urmare, măsurile de atenuare ar trebui să acopere și rețelele 4G pe care se bazează implementarea tehnologiei 5G.

(155) Pentru a aborda provocările importante în materie de securitate a rețelelor 5G, statele membre, în cadrul Grupului de cooperare NIS, împreună cu Comisia și ENISA, au efectuat o evaluare coordonată la nivelul Uniunii a riscurilor în materie de securitate ale rețelelor 5G, examinând atât riscurile tehnice, cât și pe cele non-tehnice. Această evaluare a identificat mai multe riscuri, inclusiv interferențe potențiale din partea țărilor terțe sau a actorilor din țări terțe prin intermediul lanțului de aprovizionare, și a clasificat activele în funcție de caracterul lor critic. Această evaluare ar trebui să constituie baza pentru definirea activelor TIC esențiale pentru rețelele de comunicații 5G.

(156) Pentru a atenua riscurile identificate în evaluarea coordonată la nivelul Uniunii a riscurilor în materie de securitate ale rețelelor 5G, Grupul de cooperare NIS a adoptat setul de instrumente al UE privind securitatea cibernetică a rețelelor 5G, stabilind măsuri strategice și tehnice. Deși majoritatea statelor membre dispun de cadre juridice care permit restricții sau excluderi ale furnizorilor cu grad ridicat de risc, astfel cum se recomandă în setul de instrumente pentru 5G, punerea în aplicare a cadrelor respective nu a fost uniformă. Acest lucru are ca rezultat aprovizionarea unui număr important de situri 5G din întreaga Uniune de către furnizori cu grad ridicat de risc, astfel cum se menționează în Comunicarea Comisiei privind punerea în aplicare a setului de instrumente pentru rețelele 5G[69]. Această situație creează vulnerabilități, inclusiv dependență strategică și expunere potențială la interferențe din partea țărilor terțe, care ar putea afecta, de asemenea, viitoarea infrastructură 6G construită pe rețelele 5G existente. Punerea în aplicare fragmentată a măsurilor recomandate în setul de instrumente pentru rețelele 5G, în special în ceea ce privește domeniul de aplicare al restricțiilor impuse furnizorilor cu grad ridicat de risc, a condus la divergențe între statele membre, ceea ce duce la condiții de concurență inegale, care divizează piața internă și slăbesc securitatea generală a rețelelor. Curtea de Conturi Europeană a

[69] Comunicarea Comisiei privind punerea în aplicare a setului de instrumente pentru securitatea cibernetică a rețelelor 5G, 15 iunie 2023, C(2023) 4049 final.

evidențiat aceste disparități, avertizând că absența unei abordări coordonate subminează funcționarea pieței interne. Dependența persistentă de furnizorii cu grad ridicat de risc prezintă riscuri grave pentru securitatea infrastructurii critice din Uniune și ar putea eroda încrederea în piața internă, deoarece nivelurile inconsecvente de securitate pot descuraja consumatorii și întreprinderile să se bazeze pe produse și servicii bazate pe tehnologia 5G în întreaga Uniune. Prin urmare, este esențial să existe măsuri la nivelul Uniunii pentru a asigura o abordare armonizată a securității rețelelor 5G.

(157) În scopul stabilirii unei perioade de eliminare treptată a activelor TIC esențiale ale rețelelor de comunicații electronice fixe și prin satelit, Comisia ar trebui să efectueze o evaluare care să țină seama în mod corespunzător de gradul riscurilor de securitate legate de fiecare dintre activele TIC esențiale specifice ale rețelelor fixe și prin satelit, de durata de viață a componentelor relevante și de impactul economic pe care eliminarea componentelor respective l-ar avea asupra operatorilor în cauză. Pe baza rezultatelor evaluării respective, Comisia poate lua în considerare stabilirea unor perioade diferite de eliminare treptată a anumitor active TIC esențiale și a elementelor lor integrale.

(158) În scopul supravegherii și al asigurării eficace a respectării obligațiilor privind furnizorii de rețele de comunicații electronice mobile, fixe și prin satelit, autoritățile competente relevante în temeiul prezentului regulament ar trebui să asigure o cooperare strânsă cu autoritățile competente în temeiul [propunerii DNA]. La cererea unei autorități competente desemnate în temeiul prezentului regulament, autoritățile naționale de reglementare sau alte autorități competente pentru spectrul de frecvențe radio, după caz, ar trebui să retragă drepturile menționate la articolele 9 și 20 din [propunerea DNA] în cazul în care furnizorul de rețele publice de comunicații electronice nu respectă obligațiile prevăzute în prezentul regulament, inclusiv în cazul în care furnizorul nu elimină treptat componentele TIC sau componentele care includ componente TIC de la furnizorii cu grad ridicat de risc în ceea ce privește exploatarea activelor TIC esențiale în perioada specificată în conformitate cu prezentul regulament.

(159) Având în vedere diferențele dintre structurile naționale de guvernanță, statele membre ar trebui să desemneze sau să instituie una sau mai multe autorități competente responsabile cu măsurile de supraveghere și de asigurare a respectării legislației în temeiul prezentului regulament.

(160) Autoritățile competente ar trebui să ofere sprijin entităților de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555 pentru respectarea obligațiilor care le revin în temeiul prezentului regulament. În acest scop, Comisia ar trebui să evalueze dacă furnizorii care pot fi afectați de interdicții specifice sunt stabiliți într-o țară terță care ridică motive de îngrijorare în materie de securitate cibernetică sau sunt controlați de o astfel de țară terță sau de o entitate stabilită într-o astfel de țară terță sau de un resortisant al unei astfel de țări terțe. Autoritățile competente ar trebui să coopereze îndeaproape cu Comisia și cu alte autorități competente din cadrul rețelei instituite în temeiul prezentului regulament. Pe baza evaluării efectuate de Comisie, autoritățile competente ar trebui să facă schimb de informații relevante privind furnizorii cu grad ridicat de risc cu entitățile relevante de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555. Entitățile nu trebuie să verifice dacă un furnizor se află sub control străin, dar se pot baza în totalitate pe informațiile primite de la autoritățile competente. Autoritățile competente ar trebui să se asigure că entităților respective nu li se impune nicio sarcină administrativă inutilă.

(161) Pentru a asigura respectarea efectivă, prezentul regulament ar trebui să prevadă măsuri de supraveghere și de asigurare a respectării legislației prin care autoritățile competente să poată supraveghea entitățile de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555. În cazul în care autoritățile competente își îndeplinesc sarcinile de supraveghere și de asigurare a respectării legislației în legătură cu entitățile respective, acestea nu ar trebui să depășească ceea ce este necesar și să fie proporționale cu riscurile identificate.

(162) Pentru ca asigurarea respectării normelor să fie eficace și coerentă în întreaga Uniune, este necesar să se prevadă competențe de asigurare a respectării normelor pe care autoritățile competente să le poată exercita pentru încălcarea obligațiilor prevăzute în prezentul regulament. Atunci când își exercită aceste competențe de asigurare a respectării legislației, autoritățile competente ar trebui să țină seama în mod corespunzător de o serie de factori, inclusiv de natura, gravitatea și durata încălcării, de prejudiciile materiale sau morale cauzate, de caracterul intenționat al încălcării sau de comiterea din neglijență a încălcării, de acțiunile întreprinse pentru a preveni sau a atenua prejudiciul material sau moral, de gradul de responsabilitate sau de orice încălcare anterioară relevantă, de gradul de cooperare cu autoritatea competentă și de orice alt factor agravant sau atenuant. Măsurile de asigurare a respectării legii, inclusiv sancțiunile, ar trebui să fie proporționale, iar aplicarea lor ar trebui să facă obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu Carta drepturilor fundamentale a Uniunii Europene, inclusiv dreptul la o cale de atac eficientă și la un proces echitabil, prezumția de nevinovăție și dreptul la apărare.

(163) Este important să se prevadă, de asemenea, competența de a impune daune cominatorii pentru a obliga o entitate de tipul celor menționate în anexa I sau II la Directiva (UE) 2022/2555 să înceteze o încălcare a prezentului regulament, în conformitate cu o decizie prealabilă a autorității competente.

(164) Pentru a asigura respectarea efectivă a obligațiilor prevăzute în prezentul regulament, fiecare autoritate competentă ar trebui să aibă competența de a aplica sau de a solicita aplicarea de sancțiuni.

(165) În scopul impunerii de sancțiuni unei entități de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555 care este o întreprindere, o întreprindere ar trebui înțeleasă ca fiind o întreprindere în conformitate cu articolele 101 și 102 din TFUE. În cazul în care o amendă se aplică unei persoane care nu este o întreprindere, autoritatea competentă ar trebui să țină seama de nivelul general al veniturilor din statul membru respectiv, precum și de situația economică a persoanei atunci când estimează cuantumul adecvat al sancțiunilor. Competența de a stabili dacă și în ce măsură autoritățile publice ar trebui să facă obiectul unor sancțiuni ar trebui să revină statelor membre. Aplicarea unei sancțiuni nu ar trebui să afecteze aplicarea altor competențe ale autorităților competente.

(166) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentului regulament, ar trebui conferite competențe de executare Comisiei în ceea ce privește adoptarea de acte de punere în aplicare care să stabilească norme detaliate referitoare la taxele percepute de ENISA, acte de punere în aplicare care să prevadă un sistem european de certificare a securității cibernetice pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura de securitate cibernetică a entităților, acte de punere în aplicare care să stabilească principii comune și dispoziții de referință menite să prevadă elemente în cadrul sistemelor europene de certificare a

securității cibernetice, acte de punere în aplicare care să precizeze procedurile de aprobare prealabilă sau modelele generale de delegare, acte de punere în aplicare privind recunoașterea certificatelor de securitate cibernetică ale unei țări terțe sau ale unei organizații internaționale ca fiind echivalente cu certificatele europene de securitate cibernetică, acte de punere în aplicare care să stabilească un plan de evaluare *inter pares*, acte de punere în aplicare pentru a stabili procedurile, inclusiv privind cooperarea transfrontalieră, de autorizare a organismelor de evaluare a conformității, acte de punere în aplicare pentru a stabili circumstanțele, formatele și procedurile de notificare a organismelor de evaluare a conformității, acte de punere în aplicare care desemnează o țară terță ca prezentând motive de îngrijorare legate de securitatea cibernetică la nivelul lanțurilor de aprovizionare TIC, acte de punere în aplicare prin care să se identifice activele TIC esențiale utilizate pentru fabricarea de produse sau furnizarea de servicii de către entități de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555, acte de punere în aplicare care stabilesc faptul că entitățile care își desfășoară activitatea în sectoare cu o importanță critică ridicată și în alte sectoare critice fac obiectul unor măsuri de atenuare specifice și care specifică perioadele de timp pentru eliminarea treptată a componentelor TIC sau a componentelor TIC care includ componente TIC furnizate de furnizori cu grad ridicat de risc, acte de punere în aplicare care detaliază condițiile privind derogarea pentru entitățile stabilite în țări terțe sau controlate de entități dintr-o țară terță care prezintă motive de îngrijorare în materie de securitate cibernetică, precum și adoptarea de acte de punere în aplicare care stabilesc norme detaliate referitoare la taxele percepute de Comisie. Competențele respective ar trebui să fie exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului și ar trebui utilizată procedura de examinare. În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentului regulament, Comisiei ar trebui să i se confere, de asemenea, competențe de executare în ceea ce privește stabilirea unei liste a furnizorilor cu grad ridicat de risc relevanți pentru anumite măsuri prevăzute în prezentul regulament.

(167) Este necesar ca sistemele europene de certificare a securității cibernetice să reflecte cele mai recente evoluții tehnologice, noile amenințări conexe și adoptarea unei noi legislații a Uniunii care să stabilească demonstrarea conformității și prezumția de conformitate prin certificarea europeană a securității cibernetice cu cerințele de securitate cibernetică relevante din legislația respectivă. Din aceste motive, competența de a adopta acte în conformitate cu articolul 290 din TFUE ar trebui delegată Comisiei pentru a adăuga sau a modifica obiectivele de securitate urmărite de sistemele europene de certificare a securității cibernetice. În mod similar, în interesul unui cadru fiabil privind lanțul de aprovizionare TIC, competența de a adopta acte în conformitate cu articolul 290 din TFUE ar trebui delegată Comisiei pentru a modifica anexa II la prezentul regulament în vederea adaptării acesteia la evoluțiile tehnologice. Este deosebit de important ca, în cursul activității sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile prevăzute în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare. În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul ar trebui să primească toate documentele în același timp cu experții din statele membre, iar experții acestor instituții ar trebui să aibă acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

(168) Funcționarea ENISA ar trebui să facă obiectul unei evaluări periodice și independente. Evaluarea ar trebui să țină seama de îndeplinirea de către ENISA a obiectivelor sale și

de relevanța atribuțiilor sale, mai ales a atribuțiilor legate de cooperarea operațională la nivelul Uniunii. În cazul unei revizuiri, Comisia ar trebui să evalueze modul în care poate fi consolidat rolul ENISA ca punct de referință pentru consiliere și expertiză.

(169) Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei stabilește norme în ceea ce privește adoptarea sistemului european de certificare a securității cibernetice bazat pe criterii comune (EUCC). EUCC este primul și singurul sistem european de certificare a securității cibernetice adoptat în temeiul Regulamentului (UE) 2019/881. Aceasta se referă la certificarea produselor TIC, inclusiv a produselor care aparțin domeniilor tehnice „carduri inteligente și dispozitive similare” și „dispozitive hardware cu casete de securitate”, precum și profiluri de protecție (ca procese TIC). Prin urmare, este necesar să se asigure continuarea activităților de certificare, precum și a activităților agenției.

(170) Autoritatea Europeană pentru Protecția Datelor și Comitetul european pentru protecția datelor au fost consultate în conformitate cu articolul 42 alineatul (2) din Regulamentul (UE) 2018/1725[70] și au emis un aviz comun la [data],

(171) Regulamentul (UE) 2019/881 ar trebui abrogat.

(172) Întrucât obiectivele prezentului regulament nu pot fi realizate în mod satisfăcător de către statele membre, dar, având în vedere amploarea sau efectele sale, acestea pot fi realizate mai bine la nivelul Uniunii, aceasta poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană (TUE). În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru realizarea acestor obiective,

ADOPTĂ PREZENTUL REGULAMENT:

TITLUL I
DISPOZIȚII GENERALE

Articolul 1
Obiect și domeniu de aplicare

(1) Prezentul regulament stabilește:

(a) misiunea, obiectivele, sarcinile și aspectele organizatorice legate de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA);

(b) un cadru pentru instituirea de sisteme europene de certificare a securității cibernetice cu scopul de a asigura un nivel adecvat de securitate cibernetică a produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate sau a posturii de securitate cibernetică a entităților în Uniune, precum și cu scopul de a evita fragmentarea pieței interne în ceea ce privește sistemele de certificare a securității cibernetice din Uniune și

(c) un cadru privind lanțurile de aprovizionare TIC de încredere.

---

[70] Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(2) Cadrul menționat la alineatul (1) litera (b) se aplică fără a aduce atingere dispozițiilor specifice cuprinse în alte acte juridice ale Uniunii privind certificarea voluntară sau obligatorie.

(3) Cadrul menționat la primul paragraf litera (c) se aplică entităților publice sau private de tipul celor menționate în anexa I sau II la Directiva (UE) 2022/2555 care își prestează serviciile sau își desfășoară activitățile în Uniune.

(4) Prezentul regulament nu aduce atingere funcțiilor esențiale ale statelor membre, incluzând asigurarea integrității teritoriale a statului, menținerea ordinii publice și apărarea securității naționale. În special, securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat membru.

Articolul 2
Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „securitate cibernetică” înseamnă activitățile necesare pentru protejarea rețelelor și a sistemelor informatice, a utilizatorilor unor astfel de sisteme și a altor persoane afectate de amenințări cibernetice;

2. „entități ale Uniunii” înseamnă entități ale Uniunii astfel cum sunt definite la articolul 3 punctul 1 din Regulamentul (UE, Euratom) 2023/2841;

3. „furnizor de atestate autorizat” înseamnă o entitate, publică sau privată, pentru care ENISA a adoptat o decizie de autorizare a entității respective să elibereze atestate europene individuale de competențe în materie de securitate cibernetică, astfel cum se prevede într-un sistem de atestare europeană individuală a competențelor în materie de securitate cibernetică;

4. „atestare individuală europeană a competențelor în materie de securitate cibernetică” înseamnă o înregistrare, în format digital sau fizic, care atestă că o persoană știe, înțelege și este în măsură să îndeplinească sarcinile asociate unui profil de rol sau unui subset de profiluri de rol din Cadrul european de competențe în materie de securitate cibernetică („ECSF”), în urma unei evaluări, astfel cum se prevede într-un sistem european de atestare individuală a competențelor în materie de securitate cibernetică;

5. „sistem european de atestare individuală a competențelor în materie de securitate cibernetică” înseamnă un set cuprinzător de norme, cerințe, standarde și proceduri stabilite de ENISA și asociate unui profil de rol al ECSF sau unui subset al acestuia, care se aplică furnizorilor de atestate autorizați și sunt aplicate de aceștia;

6. „rețea și sistem informatic” înseamnă rețea și sistem informatic astfel cum sunt definite la articolul 6 punctul 1 din Directiva (UE) 2022/2555;

7. „strategie națională de securitate cibernetică” înseamnă o strategie națională de securitate cibernetică astfel cum este definită la articolul 6 punctul 4 din Directiva (UE) 2022/2555;

8. „incident” înseamnă un incident în sensul definiției de la articolul 6 punctul 6 din Directiva (UE) 2022/2555;

9. „incident de securitate cibernetică de mare amploare” înseamnă un incident de securitate cibernetică de mare amploare în sensul definiției de la articolul 6 punctul 7 din Directiva (UE) 2022/2555;

10. „gestionarea incidentului” înseamnă gestionarea incidentului astfel cum este definită la articolul 6 punctul 8 din Directiva (UE) 2022/2555;

11. „amenințare cibernetică” înseamnă orice circumstanță, eveniment sau acțiune potențială care ar putea cauza daune sau perturbări la nivelul rețelelor și al sistemelor informatice, precum și la nivelul utilizatorilor unor astfel de sisteme și al altor persoane, sau care poate avea un alt fel de impact negativ asupra acestora;

12. „sistem european de certificare a securității cibernetice” înseamnă un set cuprinzător de norme, cerințe tehnice, standarde și proceduri, instituite la nivelul Uniunii, care se aplică certificării sau evaluării conformității anumitor produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate sau posturii de securitate cibernetică a entităților;

13. „sistem național de certificare a securității cibernetice” înseamnă un set cuprinzător de norme, cerințe tehnice, standarde și proceduri elaborate și adoptate de o autoritate națională publică, care se aplică certificării sau evaluării conformității produselor TIC, serviciilor TIC, proceselor TIC, serviciilor de securitate gestionate sau posturii de securitate cibernetică a entităților care intră în domeniul de aplicare al sistemului în cauză;

14. „certificat european de securitate cibernetică” înseamnă un document emis de un organism relevant prin care se atestă că un anumit produs TIC, serviciu TIC, proces TIC sau serviciu de securitate gestionat sau postura de securitate cibernetică a unei entități a fost evaluat(ă) în scopul verificării conformității cu cerințele de securitate specifice prevăzute în cadrul unui sistem european de certificare a securității cibernetice;

15. „declarație de conformitate UE” înseamnă un document emis de un producător sau de un furnizor de produse TIC, de servicii TIC, de procese TIC, de servicii de securitate gestionate sau de entitatea a cărei postură de securitate cibernetică face obiectul certificării, care atestă că îndeplinirea cerințelor corespunzătoare nivelului de asigurare „de bază”, prevăzute în sistemul european de certificare a securității cibernetice, a fost demonstrată prin autoevaluarea conformității;

16. „produs TIC” înseamnă un element sau un grup de elemente al unei rețele sau al unui sistem informatic;

17. „serviciu TIC” înseamnă un serviciu care constă integral sau preponderent în transmiterea, stocarea, extragerea sau prelucrarea informației prin intermediul rețelelor și al sistemelor informatice;

18. „proces TIC” înseamnă un set de activități desfășurate pentru a concepe, a dezvolta, a furniza sau a întreține un produs TIC sau un serviciu TIC;

19. „serviciu de securitate gestionat” înseamnă un serviciu furnizat unei părți terțe care constă în desfășurarea sau furnizarea de asistență pentru activități legate de gestionarea riscurilor în materie de securitate cibernetică, cum ar fi gestionarea incidentelor, testele de rezistență la intruziuni, auditurile de securitate și consultanța, inclusiv consultanța de specialitate în legătură cu asistența tehnică;

20. „acreditare” înseamnă acreditare astfel cum este definită la articolul 2 punctul 10 din Regulamentul (CE) nr. 765/2008;

21. „organism național de acreditare” înseamnă un organism național de acreditare astfel cum este definit la articolul 2 punctul 11 din Regulamentul (CE) nr. 765/2008;

22. „evaluarea conformității” înseamnă evaluarea conformității în sensul definiției de la articolul 2 punctul 12 din Regulamentul (CE) nr. 765/2008;

23. „organism de evaluare a conformității” înseamnă un organism de evaluare a conformității în sensul definiției de la articolul 2 punctul 13 din Regulamentul (CE) nr. 765/2008;

24. „standard” înseamnă standard în sensul definiției de la articolul 2 punctul 1 din Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului[71];

25. „specificație tehnică” înseamnă o specificație tehnică astfel cum este definită la articolul 2 punctul 4 din Regulamentul (UE) nr. 1025/2012;

26. „standard armonizat” înseamnă un standard armonizat în sensul definiției de la articolul 2 punctul 1 litera (c) din Regulamentul (UE) nr. 1025/2012;

27. „nivel de asigurare” înseamnă temeiul încrederii că un produs TIC, un serviciu TIC, un proces TIC, un serviciu de securitate gestionat sau postura de securitate cibernetică a unei entități întrunește cerințele de securitate ale unui sistem european de certificare a securității cibernetice specific și indică nivelul la care a fost evaluat(ă) un produs TIC, un serviciu TIC, un proces TIC, un serviciu de securitate gestionat sau postura de securitate cibernetică a entității, dar care nu măsoară ca atare securitatea produsului TIC, a serviciului TIC, a procesului TIC, a serviciului de securitate gestionat sau a posturii de securitate cibernetică a entității în cauză;

28. „autoevaluare a conformității” înseamnă o acțiune desfășurată de un producător sau de un furnizor de produse TIC, de servicii TIC, de procese TIC, de servicii de securitate gestionate sau entitatea a cărei postură de securitate cibernetică face obiectul certificării, care evaluează dacă respectivele produse TIC, servicii TIC, procese TIC, servicii de securitate gestionate sau posturi de securitate cibernetică ale entităților îndeplinesc cerințele unui sistem european de certificare a securității cibernetice specific;

29. „postură de securitate cibernetică a entităților” înseamnă nivelul de securitate cibernetică al entităților în ceea ce privește cerințele de securitate specifice;

30. „model de aprobare prealabilă” înseamnă un model prin care un organism de evaluare a conformității poate elibera un certificat european de securitate cibernetică pe baza evaluării de către o autoritate națională de certificare a securității cibernetice în contextul unui proces de certificare specific în cadrul unui sistem relevant;

31. „model general de delegare” înseamnă un model prin care un organism de evaluare a conformității poate elibera un certificat european de securitate cibernetică pe baza unei delegări a activităților de certificare de către o autoritate națională de certificare a securității cibernetice;

---

[71] Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului (JO L 316, 14.11.2012, p. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(32) „echipă de intervenție în caz de incidente de securitate informatică” sau „echipă CSIRT” înseamnă o echipă CSIRT desemnată sau instituită în temeiul articolului 10 din Directiva (UE) 2022/2555;

(33) „componente TIC” înseamnă produse TIC, servicii TIC sau procese TIC care pot fi utilizate în operarea activelor TIC;

(34) „active TIC” înseamnă active software sau hardware din rețeaua și sistemele informatice utilizate de o entitate de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555;

(35) „active TIC esențiale” înseamnă active TIC identificate în conformitate cu articolul 102;

(36) „rețea de comunicații electronice” înseamnă o rețea de comunicații electronice astfel cum este definită la articolul 2 punctul 1 din Regulamentul (UE) XX/XXXX [propunerea DNA];

37. „control” înseamnă capacitatea de a exercita o influență decisivă asupra unei entități juridice în mod direct sau indirect, prin intermediul uneia sau mai multor entități juridice intermediare;

38. „stabilire” înseamnă exercitarea efectivă a activității prin intermediul unor acorduri stabile în țara în care entitatea își are administrația centrală sau locul principal de desfășurare a activității;

39. „furnizor cu grad ridicat de risc” înseamnă oricare dintre următoarele:

(a) o entitate stabilită într-o țară terță care prezintă motive de îngrijorare în materie de securitate cibernetică desemnată în conformitate cu articolul 100 sau controlată de o astfel de țară terță, de o entitate stabilită într-o astfel de țară terță sau de un resortisant al unei astfel de țări terțe;

(b) o entitate desemnată în conformitate cu articolul 103 alineatul (7) și entitățile controlate de entitatea respectivă;

40. „lanț de aprovizionare TIC” înseamnă o sumă de servicii TIC, de produse TIC și de procese TIC care cuprinde activități și actori implicați în toate etapele premergătoare punerii la dispoziție a unui produs sau furnizării unui serviciu pe piață;

41. „țară terță” înseamnă o țară terță astfel cum este definită la articolul 3 alineatul (4) din Regulamentul (UE) 2023/2675 al Parlamentului European și al Consiliului[72];

42. „risc non-tehnic” înseamnă probabilitatea ca furnizorul să fie supus influenței unei țări terțe cu potențialul de a cauza pierderea sau perturbarea serviciului furnizat sau de a compromite produsul fabricat de o entitate sau de a conduce la exfiltrarea datelor, inclusiv în scopul spionajului sau al generării de venituri;

43. „risc non-tehnic semnificativ în materie de securitate cibernetică” înseamnă un risc de securitate cibernetică despre care se poate presupune că are o probabilitate ridicată de producere a unui incident care ar putea conduce la un impact negativ grav, inclusiv prin cauzarea unor perturbări sau a unor prejudicii materiale sau morale considerabile;

[72] Regulamentul (UE) 2023/2675 al Parlamentului European și al Consiliului din 22 noiembrie 2023 privind protejarea Uniunii și a statelor membre ale acesteia împotriva constrângerilor economice exercitate de țările terțe (JO L, 2023/2675, 7.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2675/oj).

44. „funcții de rețea nucleu ale rețelelor de comunicații electronice mobile” înseamnă elementul arhitectural central al rețelelor mobile de comunicații electronice care conectează principalele noduri de rețea la internet și gestionează funcțiile esențiale ale sistemului, care includ autentificarea echipamentelor utilizatorilor, funcțiile de interceptare legală (LI), gateway-urile de securitate (SeGW) la marginea rețelei, funcțiile de securitate a semnalizării, gestionarea roamingului și a sesiunilor, transmiterea de date ale utilizatorilor și ale avioanelor de control, gestionarea politicii de acces, înregistrarea și autorizarea serviciilor de rețea, stocarea datelor utilizatorilor finali și a datelor de rețea, serviciile de rețea critice, inclusiv sistemul de nume de domenii (DNS), interconectarea cu rețelele mobile ale terților, expunerea funcțiilor rețelei centrale la aplicații externe, precum și selectarea și gestionarea segmentelor de rețea;

45. „virtualizarea funcțiilor de rețea (NFV) și gestionarea și orchestrarea rețelelor de comunicații electronice mobile (MANO)” înseamnă software-ul și cadrul arhitectural care asigură gestionarea ciclului de viață, orchestrarea și automatizarea funcțiilor de rețea virtualizate (VNF), a funcțiilor de rețea native de tip cloud (CNF) și selectarea și gestionarea segmentelor de rețea în cadrul rețelelor de comunicații electronice mobile;

46. „rețea de acces radio (RAN) a rețelelor de comunicații electronice mobile” înseamnă rețeaua care conectează echipamentele utilizatorilor mobili la rețeaua nucleu, inclusiv stațiile de bază (eNodeB pentru 4G, gNodeB pentru 5G), capetele radio la distanță (RRH) și unitățile de bandă de bază (BBU), sistemele de antene active (AAS) și, după caz, componentele RAN dezagregate, cum ar fi unitățile centralizate (CU) și unitățile distribuite (DU), precum și controlerul inteligent RAN (RIC);

47. „funcții de rețea nucleu ale rețelelor de comunicații electronice fixe” înseamnă informațiile de bază ale rețelei, care conectează nodurile principale și gestionează o serie de funcții esențiale, inclusiv autentificarea și autorizarea utilizatorilor (AAA), funcțiile de interceptare legală (LI), sistemul de nume de domenii (DNS) și serviciile de adrese IP (DHCP), gestionarea politicii de acces, stocarea datelor privind utilizatorii finali și rețeaua, comutarea și rutarea IP și gateway-urile internaționale de internet (IIG);

48. „sistem de gestionare a rețelei de rețele de comunicații electronice fixe” înseamnă toate platformele centralizate și componentele software necesare pentru exploatarea, administrarea, întreținerea și furnizarea (OAM & P) rețelei și pentru monitorizarea informațiilor legate de rețea;

49. „funcții de transport și transmisie ale rețelelor de comunicații electronice fixe” înseamnă toate componentele necesare pentru backhaul și agregarea traficului în întreaga rețea, inclusiv echipamentele optice de transport, legăturile de microunde și sistemele de cabluri submarine care includ echipamentele subacvatice, precum și echipamentele terminale pentru liniile submarine (SLTE) și instalațiile fizice ale stațiilor de debarcare;

50. „rețea de acces la rețelele de comunicații electronice fixe” înseamnă rețeaua care conectează amplasamentul utilizatorului final la agregare sau la rețeaua nucleu, inclusiv terminația liniei optice (OLT) și terminația rețelei optice (ONT) pentru rețelele de fibră optică; sistem de terminare a modemului coaxial de cablu (CMTS) și modemuri de cablu pentru rețelele de cablu coaxial, precum și componente fixe de acces fără fir, în cazul în care sunt utilizate ca substitut de linie fixă.

TITLUL II
AGENȚIA UNIUNII EUROPENE PENTRU SECURITATE CIBERNETICĂ

Capitolul I
Misiune și obiective

Articolul 3
Misiunea ENISA

(1) Misiunea ENISA este de a sprijini statele membre și entitățile Uniunii în atingerea unui nivel ridicat de securitate cibernetică, reziliență cibernetică și încredere în Uniune.

(2) ENISA acționează ca punct de referință pentru consiliere și expertiză în materie de securitate cibernetică pentru statele membre, precum și pentru alte părți interesate din Uniune.

(3) ENISA contribuie la reducerea fragmentării pe piața internă prin îndeplinirea atribuțiilor care îi sunt încredințate în temeiul prezentului regulament.

(4) ENISA îndeplinește sarcinile care îi sunt atribuite prin acte juridice ale Uniunii.

(5) ENISA își dezvoltă propriile capacități, inclusiv capacitățile și competențele tehnice și umane, necesare pentru a îndeplini atribuțiile care îi sunt încredințate în temeiul prezentului regulament.

Articolul 4
Obiectivele ENISA

(1) ENISA este un centru de expertiză în materie de securitate cibernetică, datorită independenței sale, calității științifice și tehnice a consilierii, contribuțiilor și asistenței acordate și a informațiilor furnizate, transparenței procedurilor de operare și metodelor de funcționare, precum și a diligenței cu care își îndeplinește atribuțiile.

(2) ENISA asistă statele membre și, după caz, entitățile Uniunii în punerea în aplicare a politicilor orizontale și sectoriale ale Uniunii și a legislației legate de securitatea cibernetică, inclusiv a activităților de supraveghere a pieței.

(3) ENISA își pune la dispoziție expertiza și asistă Comisia în elaborarea politicilor și a legislației Uniunii referitoare la securitatea cibernetică.

(4) ENISA sprijină consolidarea capacităților și pregătirea în întreaga Uniune, oferind asistență statelor membre, entităților Uniunii, prin intermediul Serviciului de securitate cibernetică pentru instituțiile, organele, oficiile și agențiile Uniunii (CERT-UE) menționat în capitolul IV din Regulamentul (UE, Euratom) 2023/2841, precum și părților interesate din sectorul public și privat pentru a spori protecția rețelelor și a sistemelor lor informatice, pentru a dezvolta și a îmbunătăți reziliența cibernetică și capacitățile de răspuns.

(5) ENISA contribuie la punerea în aplicare a Academiei de competențe în materie de securitate cibernetică și la creșterea forței de muncă din domeniul securității cibernetice în Uniune prin sprijinirea eforturilor de dezvoltare a portabilității competențelor în întreaga Uniune, inclusiv prin întreținerea și promovarea adoptării

ECSF și prin dezvoltarea, întreținerea și promovarea adoptării sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică în conformitate cu capitolul II secțiunea 4 din prezentul titlu, precum și prin asigurarea furnizării de formare în conformitate cu articolul 6 alineatul (8).

(6) ENISA promovează cooperarea, inclusiv schimbul de informații și coordonarea la nivelul Uniunii, între statele membre, entitățile Uniunii în conformitate cu Regulamentul (UE, Euratom) 2023/2841 și părțile interesate relevante din sectorul public și privat cu privire la aspecte legate de securitatea cibernetică.

(7) ENISA contribuie la sporirea capacităților de securitate cibernetică la nivelul Uniunii pentru a sprijini acțiunile statelor membre în materie de prevenire a amenințărilor cibernetice și de răspuns la acestea.

(8) ENISA sprijină cooperarea operațională la nivelul Uniunii, inclusiv prin contribuția la conștientizarea comună a situației amenințărilor și incidentelor cibernetice în rândul statelor membre și, în cooperare cu CERT-UE, în rândul entităților Uniunii.

(9) ENISA cooperează îndeaproape cu Europol, CSIRT și alte autorități naționale relevante pentru a îmbunătăți pregătirea și răspunsul în materie de securitate cibernetică la incidentele de tip ransomware.

(10) ENISA contribuie la instituirea și menținerea unui cadru european de certificare a securității cibernetice în conformitate cu titlul III din prezentul regulament. ENISA promovează recurgerea la certificarea europeană a securității cibernetice, cu scopul de a evita fragmentarea pieței interne.

(11) ENISA contribuie la armonizarea pieței unice digitale prin implicarea în activități de standardizare relevante pentru politicile Uniunii legate de securitatea cibernetică și prin elaborarea de specificații tehnice.

(12) ENISA promovează un nivel ridicat de sensibilizare în materie de securitate cibernetică în rândul organizațiilor și al întreprinderilor.

Capitolul II
Sarcini

Secțiunea 1
Sprijin pentru punerea în aplicare a politicii și legislației Uniunii

Articolul 5
Sprijin pentru punerea în aplicare a politicii și legislației Uniunii

(1) ENISA contribuie la punerea în aplicare a politicii și a legislației Uniunii:

(a) acordând asistență statelor membre în punerea în aplicare consecventă a politicii și a legislației Uniunii în materie de securitate cibernetică, inclusiv prin emiterea de orientări tehnice și de rapoarte, prin furnizarea de consiliere și schimbul de bune practici și prin facilitarea schimbului de bune practici între autoritățile competente în această privință;

(b) sprijinind schimbul de informații în cadrul sectoarelor și între acestea, în special în ceea ce privește sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555 și produsele cu elemente digitale care intră în domeniul de

aplicare al Regulamentului (UE) 2024/2847, prin furnizarea de bune practici și orientări privind instrumentele și procedurile disponibile;

(c) la cererea Comisiei, acordând asistență statelor membre prin furnizarea de sprijin, cum ar fi orientări tehnice, inclusiv cu privire la măsurile de gestionare a riscurilor în materie de securitate cibernetică, instrumente de evaluare a maturității în materie de securitate cibernetică și manuale de răspuns la incidente, adaptate sectoarelor enumerate în anexele I și II la Directiva (UE) 2022/2555, sau sprijin pentru punerea în aplicare a principiilor de securitate cibernetică de la stadiul conceperii pentru produsele cu elemente digitale în conformitate cu Regulamentul (UE) 2024/2847, cu scopul de a facilita îmbunătățirea nivelurilor de maturitate în materie de securitate cibernetică și respectarea dreptului Uniunii în ceea ce privește securitatea cibernetică;

(d) contribuind la activitatea Grupului de cooperare instituit în temeiul articolului 14 alineatul (1) din Directiva (UE) 2022/2555 („Grupul de cooperare NIS”), a Grupului european de cooperare privind identitatea digitală instituit în temeiul articolului 46e alineatul (1) din Regulamentul (UE) nr. 910/2014, a Grupului european pentru certificarea securității cibernetice („ECCG”), astfel cum se menționează la articolul 90 din prezentul regulament, și a Grupului de cooperare administrativă (ADCO) instituit în temeiul articolului 52 alineatul (15) din Regulamentul (UE) 2024/2847;

(e) acordând asistență statelor membre și entităților relevante ale Uniunii în elaborarea și promovarea politicilor de securitate cibernetică legate de susținerea disponibilității și integrității generale a nucleului public al internetului deschis;

(f) în conformitate cu Regulamentul (UE) 2024/2847, furnizând consiliere și sprijin tehnic statelor membre și Comisiei cu privire la aspecte legate de punerea în aplicare a regulamentului respectiv;

(g) acordând asistență statelor membre în ceea ce privește desfășurarea asistenței reciproce și facilitarea unor astfel de procese de cooperare pentru entitățile esențiale și importante în temeiul [articolului 37a din Directiva (UE) 2022/2555];

(h) la cererea Comitetului european pentru protecția datelor, furnizând consiliere cu privire la punerea în aplicare a aspectelor specifice de securitate cibernetică ale politicii și legislației Uniunii legate de protecția datelor și a vieții private.

(2) ENISA contribuie la evaluări coordonate ale riscurilor în materie de securitate cibernetică la nivelul Uniunii, inclusiv la cele efectuate în temeiul articolului 22 din Directiva (UE) 2022/2555.

(3) ENISA emite orientări privind interoperabilitatea rețelelor și a sistemelor informatice utilizate pentru schimbul de informații, inclusiv în ceea ce privește centrele cibernetice transfrontaliere, astfel cum se menționează la articolul 6 alineatul (3) din Regulamentul (UE) 2025/38.

(4) ENISA este membră a Grupului de cooperare NIS în temeiul articolului 14 alineatul (3) din Directiva (UE) 2022/2555.

(5) La cererea Comisiei, ENISA furnizează expertiză, consiliere tehnică, informații sau analize sau desfășoară activități pregătitoare cu privire la aspecte specifice legate de

securitatea cibernetică, cu scopul de a contribui la elaborarea politicilor Comisiei și la monitorizarea punerii în aplicare a legislației Uniunii.

Articolul 6
Consolidarea capacităților

ENISA acordă asistență:

1. statelor membre, în eforturile lor de a îmbunătăți prevenirea, detectarea și analizarea amenințărilor cibernetice și a incidentelor și capacitatea de răspuns la acestea, prin furnizarea cunoștințelor și a expertizei necesare;
2. statelor membre, la cererea acestora, în stabilirea și punerea în aplicare a politicilor de divulgare a vulnerabilităților în mod voluntar;
3. în conformitate cu Regulamentul (UE, Euratom) 2023/2841, CERT-UE și Consiliului interinstituțional pentru securitate cibernetică în eforturile lor de a sprijini entitățile Uniunii în consolidarea securității lor cibernetice, de a îmbunătăți prevenirea, detectarea și analiza amenințărilor și incidentelor cibernetice, precum și de a-și îmbunătăți capacitățile de răspuns la astfel de amenințări și incidente cibernetice;
4. statelor membre în ceea ce privește dezvoltarea echipelor CSIRT naționale, la solicitarea acestora, în temeiul articolului 10 alineatul (10) din Directiva (UE) 2022/2555;
5. statelor membre în ceea ce privește elaborarea sau actualizarea unei strategii naționale de securitate cibernetică și a indicatorilor-cheie de performanță pentru evaluarea strategiei respective, atunci când acest lucru este solicitat în temeiul articolului 7 alineatul (4) din Directiva (UE) 2022/2555, promovează difuzarea strategiilor respective și ia act de progresele înregistrate în punerea lor în aplicare în întreaga Uniune, pentru a promova cele mai bune practici;
6. instituțiilor Uniunii, la cererea acestora, în ceea ce privește elaborarea și revizuirea strategiilor Uniunii referitoare la securitatea cibernetică, promovarea difuzării acestora, precum și urmărirea progreselor înregistrate în punerea lor în aplicare;
7. echipelor CSIRT naționale, în ceea ce privește creșterea nivelului capacităților proprii, inclusiv prin promovarea dialogului și a schimbului de informații, pentru a garanta că, având în vedere stadiul actual al tehnologiei, fiecare echipă CSIRT dispune de un set comun de capacități minime și funcționează în conformitate cu cele mai bune practici;
8. statelor membre, entităților Uniunii și părților interesate din sectorul public și privat în eforturile lor de evaluare, creștere și consolidare a forței de muncă din domeniul securității cibernetice, inclusiv prin dezvoltarea, menținerea și promovarea adoptării instrumentelor relevante, cum ar fi ECSF și sistemele europene de atestare individuală a competențelor în materie de securitate cibernetică, în conformitate cu secțiunea 4 din prezentul capitol;
9. organismelor publice relevante, precum și părților interesate din sectorul privat, prin desfășurarea de cursuri de formare specifice, după caz, în cooperare cu părțile interesate;

10. Grupului de cooperare NIS în ceea ce privește schimbul de bune practici și de informații, în special în legătură cu punerea în aplicare a Directivei (UE) 2022/2555 în temeiul articolului 14 alineatul (4) litera (c) din directiva respectivă;

11. autorităților de supraveghere a pieței desemnate în temeiul Regulamentului (UE) 2024/2847 în activitățile lor care vizează asigurarea punerii în aplicare eficace a regulamentului respectiv, inclusiv sprijin pentru orientări și consiliere tehnică pentru operatorii economici, sprijin pentru verificările conformității, evaluarea riscurilor, activități comune și acțiuni de verificare, astfel cum se prevede în Regulamentul (UE) 2024/2847;

12. membrilor ECCG în schimbul de bune practici și, la cererea fiecărui stat membru, asistă autoritățile naționale de certificare a securității cibernetice în ceea ce privește punerea în aplicare a sistemelor europene de certificare a securității cibernetice la nivel național;

13. autorităților publice și părților interesate din sectorul privat în ceea ce privește activitățile de evaluare a conformității și de evaluare, inclusiv organismelor de evaluare a conformității și întreprinderilor mici și mijlocii, pentru a sprijini un ecosistem solid, competitiv, favorabil incluziunii și armonizat de evaluare a conformității care să sprijine punerea în aplicare a Regulamentului (UE) 2024/2847 și a cadrului european de certificare a securității cibernetice;

14. Centrului european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică și Rețelei de centre naționale de coordonare instituite în temeiul Regulamentului (UE) 2021/887 prin schimbul de informații cu privire la riscurile și amenințările cibernetice actuale și emergente, inclusiv în ceea ce privește tehnologiile informației și comunicațiilor noi și emergente;

15. statelor membre, prin furnizarea de sprijin tehnic, inclusiv pentru instituirea și funcționarea spațiilor de testare în materie de reglementare în domeniul securității cibernetice, în conformitate cu legislația relevantă a Uniunii.

Articolul 7
Acțiuni de sensibilizare și rezerva de talente

ENISA sprijină statele membre în eforturile lor de sensibilizare cu privire la politicile și legislația Uniunii în materie de securitate cibernetică și promovează vizibilitatea acestora prin dezvoltarea de instrumente și orientări realizabile. ENISA sprijină inițiativele care vizează creșterea rezervei europene de talente în materie de securitate cibernetică, în special prin coordonarea concursurilor.

Articolul 8
Cunoștințe și analize de piață

(1) ENISA efectuează și diseminează analize ale principalelor tendințe ale pieței securității cibernetice, atât din perspectiva cererii, cât și din perspectiva ofertei, în special în ceea ce privește domeniile în care există sau sunt planificate sisteme europene de certificare a securității cibernetice, sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555 și categoriile de produse care intră sub incidența Regulamentului (UE) 2024/2847, inclusiv anexele III și IV la regulamentul respectiv.

(2) ENISA efectuează și diseminează analize ale tendințelor tehnologice în materie de securitate cibernetică, în special în ceea ce privește activitățile și entitățile care intră în domeniul de aplicare al Directivei (UE) 2022/2555 și produsele cu elemente digitale care intră în domeniul de aplicare al Regulamentului (UE) 2024/2847.

(3) ENISA consolidează cunoștințele și diseminează consiliere tehnică și analize cu privire la instrumente, cadre, standarde și bune practici de securitate cibernetică de ultimă generație.

Articolul 9
Cooperarea internațională

ENISA contribuie la eforturile Uniunii de cooperare cu țări terțe și cu organizații internaționale, precum și în cadrele internaționale de cooperare relevante, pentru a promova cooperarea internațională privind aspecte legate de securitatea cibernetică prin:

(a) participarea ca observator la organizarea de exerciții internaționale și realizarea de analize și de rapoarte destinate consiliului de administrație privind rezultatele acestor exerciții, după caz;

(b) facilitarea, la solicitarea Comisiei, a schimbului de bune practici cu țările terțe și cu organizațiile internaționale;

(c) furnizarea de expertiză Comisiei, la cererea acesteia;

(d) furnizarea de consiliere și sprijin de specialitate Comisiei cu privire la aspecte legate de recunoașterea internațională a certificatelor europene de securitate cibernetică în conformitate cu articolul 87;

(e) furnizarea de consiliere și sprijin de specialitate Comisiei cu privire la aspecte legate de standardizarea internațională și colaborarea cu organizațiile internaționale de standardizare relevante, după caz, în colaborare cu ECCG instituit în temeiul articolului 90.

Secțiunea 2

Cooperare operațională

Articolul 10
Cooperarea operațională la nivelul Uniunii

(1) ENISA sprijină cooperarea operațională între statele membre, entitățile Uniunii prin intermediul CERT-UE și între alte părți interesate.

(2) ENISA este membră a rețelei de echipe CSIRT naționale instituite în temeiul articolului 15 alineatul (1) din Directiva (UE) 2022/2555 și asigură secretariatul rețelei CSIRT în temeiul articolului 15 alineatul (2) din Directiva (UE) 2022/2555.

(3) ENISA asigură secretariatul Rețelei europene a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe) în temeiul articolului 16 alineatul (2) al doilea paragraf din Directiva (UE) 2022/2555.

(4) ENISA sprijină cooperarea tehnică și operațională între statele membre, în special prin intermediul rețelei CSIRT și al EU-CyCLONe. Acest sprijin include:

(a) consilierea cu privire la îmbunătățirea capacităților de prevenire, detectare, răspuns și redresare în urma incidentelor;

(b) la cererea unuia sau mai multor state membre, furnizarea de consiliere și evaluări în legătură cu un anumit incident potențial sau în curs sau cu o anumită amenințare cibernetică, inclusiv prin furnizarea de expertiză și prin facilitarea gestionării tehnice a unor astfel de incidente, precum și prin sprijinirea schimbului voluntar de informații relevante și de soluții tehnice între statele membre;

(c) analizarea vulnerabilităților, a amenințărilor și a incidentelor;

(d) la cererea unuia sau mai multor state membre, furnizarea de sprijin în legătură cu anchetele tehnice *ex post* privind incidentele semnificative în sensul articolului 23 alineatul (3) din Directiva (UE) 2022/2555;

(e) contribuția la sprijinirea gestionării coordonate a incidentelor și crizelor de securitate cibernetică de mare amploare la nivel operațional, în special prin sprijinirea EU-CyCLONe în pregătirea rapoartelor către nivelul politic și prin facilitarea schimbului de informații în timp util între rețeaua CSIRT și EU-CyCLONe;

(5) La cererea unui stat membru sau a unei entități a Uniunii în cooperare cu CERT-UE, ENISA sprijină comunicarea publică coerentă cu privire la un incident sau o amenințare cibernetică.

(6) ENISA sprijină cooperarea dintre statele membre și, prin intermediul CERT-UE, dintre entitățile Uniunii în ceea ce privește implementarea instrumentelor de comunicații securizate. ENISA utilizează, în cadrul rețelei CSIRT și al EU-CyCLONe, instrumente securizate de comunicații care sunt furnizate de entități juridice stabilite sau considerate a fi stabilite în Uniune și controlate de statele membre sau de resortisanți ai statelor membre.

Articolul 11

Conștientizarea comună a situației în materie de securitate cibernetică

(1) În scopul unei mai bune conștientizări comune a situației în ceea ce privește peisajul amenințărilor și incidentelor cibernetice între statele membre și între entitățile Uniunii, ENISA:

(a) dezvoltă, în cooperare cu EU-CyCLONe, rețeaua CSIRT, Comisia, CERT-UE, Europol și alte entități relevante ale Uniunii, registre de informații verificate și fiabile privind amenințările cibernetice, inclusiv tendințele în materie de incidente, tactici, tehnici și proceduri;

(b) în conformitate cu articolul 12, emite alerte timpurii cu privire la un incident semnificativ sau de mare amploare potențial sau în curs sau la o amenințare cibernetică de natură potențial transfrontalieră, în special în ceea ce privește sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555;

(c) furnizează în timp util analize ad-hoc cu privire la tendințele emergente în materie de incidente, la cererea rețelei CSIRT, a EU-CyCLONe sau a Comisiei;

(d) furnizează, la cererea statelor membre sau a Comisiei, analize sau alte informații privind un risc sau o amenințare reală sau percepută în materie de securitate cibernetică;

(e) furnizează analize și consiliere tehnică privind riscurile de securitate cibernetică ale produselor cu elemente digitale, inclusiv pentru a sprijini supravegherea pieței și prin elaborarea unui raport tehnic bienal privind tendințele emergente, în conformitate cu articolul 17 alineatul (3) din Regulamentul (UE) 2024/2847;

(f) elaborează un raport periodic aprofundat asupra situației tehnice în materie de securitate cibernetică la nivelul UE referitor la incidente și amenințări cibernetice și pune raportul la dispoziția Consiliului, a EU-CyCLONe, a rețelei CSIRT, a Comisiei, a Serviciului European de Acțiune Externă și a Europol;

(g) monitorizează tendințele în ceea ce privește tehnicile, cererile și impactul atacurilor de tip ransomware și furnizează informații cu privire la aceste tendințe Comisiei, rețelei CSIRT și EU-CyCLONe și Europol.

(2) În scopul unei mai bune conștientizări comune a situației în ceea ce privește peisajul amenințărilor și incidentelor cibernetice în rândul părților interesate, ENISA:

(a) efectuează analize ale amenințărilor cibernetice, ale incidentelor, ale tendințelor, ale tehnologiilor emergente și ale impactului acestora, inclusiv o analiză periodică a sectoarelor enumerate în anexele I și II la Directiva (UE) 2022/2555 și a categoriilor de produse relevante care intră sub incidența Regulamentului (UE) 2024/2847;

(b) emite, în cooperare cu Comisia și, după caz, cu rețeaua CSIRT, consiliere, orientări și bune practici pentru securitatea rețelelor și a sistemelor informatice, în special pentru securitatea infrastructurilor care sprijină sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555;

(c) efectuează analize strategice pe termen lung ale amenințărilor cibernetice și incidentelor, pentru a identifica tendințele emergente și a contribui la prevenirea incidentelor;

(3) ENISA poate face publice analizele, consilierea, orientările, bunele practici și rapoartele menționate la alineatul (2), de comun acord cu entitățile contribuitoare menționate la alineatul (2).

(4) În desfășurarea activităților enumerate la alineatul (1) literele (a)-(d) și litera (f) și la alineatul (2), ENISA utilizează propriile analize și, după caz, informațiile primite în îndeplinirea sarcinilor sale, inclusiv:

(a) informațiile furnizate din surse aflate la dispoziția publicului, inclusiv vulnerabilitățile cunoscute public ale produselor TIC sau ale serviciilor TIC disponibile în baza de date europeană a vulnerabilităților instituită în temeiul articolului 12 alineatul (2) din Directiva (UE) 2022/2555;

(b) informațiile partajate de statele membre, entitățile Uniunii, CERT-UE, partenerii din sectorul privat sau neguvernamental și organizațiile din țări terțe și internaționale, sub rezerva oricăror limitări prin intermediul unui marcaj vizibil privind distribuirea ulterioară a informațiilor respective.

(5) ENISA cooperează îndeaproape cu statele membre la pregătirea raportului asupra situației tehnice în materie de securitate cibernetică la nivelul UE menționat la

alineatul (1) litera (e). Raportul se bazează pe informațiile disponibile public, pe analiza proprie a ENISA și pe rapoartele transmise, printre altele, de echipele CSIRT ale statelor membre sau de punctele unice de contact instituite prin Directiva (UE) 2022/2555, atât în mod voluntar, de EC3 și de CERT-UE. De comun acord cu entitățile contribuitoare, ENISA poate pune la dispoziția publicului o versiune agregată a raportului.

Articolul 12
Alerte timpurii

(1) Alertele timpurii menționate la articolul 11 alineatul (1) primul paragraf litera (b) din prezentul regulament conțin informații relevante privind un incident semnificativ sau de mare amploare potențial sau în curs sau o amenințare cibernetică de natură potențial transfrontalieră în legătură cu sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555. Aceste informații pot include vulnerabilități cunoscute public și dacă acestea afectează produse cu elemente digitale care intră sub incidența Regulamentului (UE) 2024/2847, tehnici și proceduri, indicatori de compromis, tactici contradictorii, informații specifice actorului care generează amenințări și recomandări privind măsurile de atenuare.

(2) Alertele timpurii menționate la articolul 11 alineatul (1) primul paragraf litera (b) se emit cât mai curând posibil către echipa CSIRT sau echipele CSIRT în cauză și, după caz, către rețeaua CSIRT și EU-CyCLONe.

(3) ENISA oferă un serviciu de alertă timpurie entităților care își desfășoară activitatea în sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555.

(4) Serviciul menționat la alineatul (3) este furnizat la cererea entității și într-un format prelucrabil automat pus la dispoziția publicului. Serviciul respectiv include schimbul de informații privind indicatorii amenințărilor cibernetice și recomandări privind măsurile de atenuare.

(5) ENISA stabilește o procedură pentru diseminarea alertelor timpurii către entitățile menționate la alineatul (3).

Articolul 13
Sprijin pentru răspunsul la incidente și revizuirea acestora

(1) ENISA operează și administrează rezerva UE pentru securitate cibernetică, integral sau parțial, în conformitate cu Regulamentul (UE) 2025/38.

(2) La cererea Comisiei sau a EU-CyCLONe, ENISA, cu sprijinul rețelei CSIRT și cu aprobarea statului membru în cauză, revizuiește și evaluează incidentele de securitate cibernetică semnificative sau incidentele de securitate cibernetică de mare amploare în conformitate cu articolul 21 din Regulamentul (UE) 2025/38.

(3) ENISA sprijină, în cooperare cu Europol și CSIRT sau cu alte autorități competente, după caz, entitățile esențiale și importante individuale enumerate în anexele I și II la Directiva (UE) 2022/2555 în pregătirea, răspunsul și redresarea în urma unui incident de tip ransomware. În acest scop, ENISA instituie un serviciu de asistență și, în special, utilizează conștientizarea comună sporită a situației în ceea ce privește peisajul amenințărilor și incidentelor cibernetice în temeiul articolului 11 alineatul (1) primul paragraf literele (a) și (g) din prezentul regulament.

Articolul 14
Exerciții de securitate cibernetică la nivelul Uniunii

(1) ENISA sprijină Comisia în elaborarea unui program anual continuu de exerciții de securitate cibernetică la nivelul Uniunii.

(2) ENISA menține un registru al învățămintelor desprinse în urma exercițiilor menționate la alineatul (1) și recomandă statelor membre și, după caz, entităților Uniunii modul în care să pună în aplicare în mod eficace și eficient învățămintele desprinse.

(3) La cererea EU-CyCLONe sau a Comisiei, ENISA organizează exerciții de securitate cibernetică la nivelul Uniunii sau contribuie la organizarea acestora, inclusiv testarea pregătirii pentru a răspunde la incidentele și crizele de securitate cibernetică de mare amploare la nivelul Uniunii.

(4) La cererea statelor membre, ENISA le sprijină în organizarea exercițiilor naționale de securitate cibernetică.

(5) La cererea CERT-UE, ENISA contribuie la organizarea exercițiilor de securitate cibernetică organizate de CERT-UE în temeiul articolului 13 alineatul (7) din Regulamentul (UE, Euratom) 2023/2841.

Articolul 15
Furnizarea de instrumente și platforme

(1) ENISA instituie, furnizează, operează, întreține și actualizează, după caz, instrumente tehnice operaționale, inclusiv platforme legate de securitatea cibernetică la nivelul Uniunii, în special platforma unică de raportare instituită în temeiul articolului 16 alineatul (1) din Regulamentul (UE) 2024/2847 [și punctul unic de intrare pentru raportarea incidentelor instituit în temeiul articolului 23a din Directiva (UE) 2022/2555], precum și instrumente de testare pentru a sprijini punerea în aplicare a procedurilor de evaluare a conformității în conformitate cu legislația relevantă a Uniunii.

(2) După caz, în sensul alineatului (1), ENISA cooperează și face schimb de informații cu rețeaua CSIRT și, după caz, cu autoritățile de supraveghere a pieței.

Articolul 16
Servicii de gestionare a vulnerabilităților

ENISA dezvoltă o capacitate comună a Uniunii de servicii de gestionare a vulnerabilităților și furnizează servicii de gestionare a vulnerabilităților părților interesate prin:

(a) întreținerea bazei de date europene a vulnerabilităților instituite în temeiul articolului 12 alineatul (2) din Directiva (UE) 2022/2555;

(b) furnizarea de servicii de gestionare a vulnerabilităților către părțile interesate, pe baza bazei de date europene a vulnerabilităților și utilizând informațiile relevante aflate la dispoziția ENISA;

(c) după caz, inițierea unei cooperări structurate cu organizații care furnizează programe, registre sau baze de date similare cu baza de date europeană a vulnerabilităților;

(d) sprijinirea activă a echipelor CSIRT desemnate drept coordonatori în temeiul articolului 12 alineatul (1) din Directiva (UE) 2022/2555 în ceea ce privește

gestionarea divulgării coordonate a vulnerabilităților care pot avea un impact semnificativ asupra entităților din mai multe state membre;

(e) dezvoltarea și menținerea metodologiilor și a mecanismelor de guvernanță pentru identificarea vulnerabilităților și divulgarea coordonată, în cooperare cu autoritățile naționale competente, echipele CSIRT, industria și comunitatea de cercetare.

Secțiunea 3

Certificarea și standardizarea securității cibernetice

Articolul 17
Certificarea securității cibernetice

(1) ENISA contribuie la elaborarea și punerea în aplicare a politicii Uniunii privind certificarea de securitate cibernetică, astfel cum se prevede în titlul III din prezentul regulament, și promovează aceste politici. ENISA este responsabilă de:

(a) pregătirea propunerilor de sisteme europene de certificare a securității cibernetice („propuneri de sisteme”) pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate și postura de securitate cibernetică a entităților în conformitate cu articolul 74 și, după caz, elaborarea de specificații tehnice în conformitate cu articolul 77;

(b) întreținerea sistemelor europene de certificare a securității cibernetice adoptate în conformitate cu articolul 75, inclusiv în vederea unei posibile revizuiri a sistemelor europene de certificare a securității cibernetice adoptate în conformitate cu articolul 76;

(c) promovarea adoptării sistemelor adoptate și menținerea unui site web dedicat care să ofere informații privind sistemele europene de certificare a securității cibernetice, certificatele europene de securitate cibernetică și declarațiile de conformitate UE în conformitate cu articolul 79 și să le facă publice;

(d) organizarea consolidării capacităților legate de procesele de certificare, activitățile de evaluare, revizuirea *inter pares* și evaluarea *inter pares*, inclusiv prin acordarea de sprijin statelor membre, la cererea acestora, în conformitate cu articolul 6 alineatul (12).

(2) ENISA sprijină Comisia în următoarele activități:

(a) guvernanța ECCG în temeiul articolului 90;

(b) organizarea unui sistem european de certificare a securității cibernetice în conformitate cu articolul 72 alineatul (1);

(c) în legătură cu recunoașterea internațională a certificatelor europene de securitate cibernetică în conformitate cu articolul 87;

(d) organizarea de evaluări *inter pares* în temeiul articolului 89;

(e) elaborarea de modele de dispoziții care să fie menționate în sistemele europene de certificare a securității cibernetice pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate și postura de securitate cibernetică a entităților, în conformitate cu articolul 81 alineatul (5).

Articolul 18
Standardizare, specificații tehnice și orientări

(1) ENISA elaborează proiecte de specificații tehnice și orientări pentru a sprijini punerea în aplicare a legislației Uniunii în domeniul securității cibernetice. La elaborarea specificațiilor tehnice respective, ENISA ia în considerare standardele europene și internaționale existente, precum și alte specificații tehnice relevante. ENISA asigură coerența specificațiilor și orientărilor sale tehnice.

(2) ENISA monitorizează și, după caz, participă și conduce activitățile de dezvoltare a standardizării la nivelul Uniunii și, în conformitate cu articolul 9, la nivel internațional, în vederea sprijinirii politicilor Uniunii legate de securitatea cibernetică.

(3) ENISA sprijină dezvoltarea și evaluarea algoritmilor criptografici. În cazul în care un algoritm criptografic este evaluat pozitiv de ENISA, ENISA cooperează, în conformitate cu Regulamentul (UE) nr. 1025/2012, cu organismele europene de standardizare pentru a sprijini standardizarea acestuia.

(4) ENISA oferă consiliere tehnică Comisiei și, după caz, statelor membre cu privire la standardele sau specificațiile tehnice adecvate în sprijinul politicilor Uniunii legate de securitatea cibernetică, inclusiv pentru legislația de armonizare a Uniunii în domeniul securității cibernetice, în special Regulamentul (UE) 2024/2847, pentru domeniile tehnice în sensul articolului 25 din Directiva (UE) 2022/2555 și pentru sistemele europene de certificare a securității cibernetice în temeiul articolului 81 alineatul (1) litera (d).

(5) ENISA asistă Comisia la evaluarea proiectelor de standarde armonizate pentru a sprijini punerea în aplicare a legislației de armonizare a Uniunii în domeniul securității cibernetice.

(6) ENISA promovează adoptarea standardelor europene și internaționale în materie de securitate cibernetică.

(7) ENISA îndeplinește sarcinile menționate la alineatele (1)-(6) cu integritate, imparțialitate și confidențialitate, inclusiv prin retragerea sau întreruperea participării sale din cadrul unor organisme tehnice specifice atunci când o astfel de participare intră în conflict cu alte sarcini sau obiective.

Secțiunea 4
Punerea în aplicare a Academiei de competențe în materie de securitate cibernetică

Articolul 19
Cadrul european de competențe în materie de securitate cibernetică

(1) ENISA elaborează și pune la dispoziția publicului un cadru european de competențe în materie de securitate cibernetică („ECSF”). Înainte de a pune ECSF la dispoziția publicului sau de a-l actualiza în temeiul alineatului (4), ENISA consultă Comisia.

(2) ECSF definește profilurile profesioniștilor din domeniul securității cibernetice și asocierea unor sarcini, competențe și cunoștințe specifice cu un anumit profil de rol. Utilizarea ECSF este voluntară pentru entitățile publice și private.

(3) ENISA poate consulta părțile interesate în dezvoltarea și adoptarea ECSF.

(4) ENISA evaluează necesitatea de a actualiza ECSF în mod regulat și, după caz, o actualizează.

Articolul 20
Dezvoltarea, adoptarea și întreținerea sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică

(1) ENISA elaborează, adoptă și menține sisteme europene de atestare individuală a competențelor în materie de securitate cibernetică. Utilizarea sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică este voluntară pentru organismele publice naționale și entitățile private, cu excepția cazului în care se prevede altfel în dreptul intern.

(2) Înainte de a iniția un nou sistem european de atestare individuală a competențelor în materie de securitate cibernetică, ENISA consultă Comisia. ENISA adoptă un astfel de sistem numai în urma unui aviz pozitiv din partea Comisiei. Atunci când pregătește un sistem european de atestare individuală a competențelor în materie de securitate cibernetică, ENISA poate consulta părțile interesate relevante.

(3) Un sistem european de atestare individuală a competențelor în materie de securitate cibernetică trebuie să includă următoarele:

(a) obiectul și domeniul de aplicare al sistemului de atestare bazat pe profilurile de rol ale ECSF sau pe subseturile acestora;

(b) cerințele aplicabile persoanelor instruite să efectueze evaluări („evaluatori”) în conformitate cu articolul 21, competențele, cunoștințele și experiența necesare, precum și metodele de formare;

(c) analiza pătrunderii pe piață specifică fiecărui sistem de atestare;

(d) rezultatele învățării, metodele de evaluare și condițiile pe care furnizorii de atestate autorizați le utilizează pentru a evalua demonstrarea de către o persoană a competențelor necesare în conformitate cu articolul 21;

(e) dacă este cazul, unul sau mai multe niveluri de competență;

(f) norme privind păstrarea evidențelor de către furnizorii de atestate autorizați;

(g) conținutul și formatul atestatelor europene individuale de competențe în materie de securitate cibernetică, ținând seama în mod corespunzător de articolul 21 alineatul (5) litera (e);

(h) perioada maximă de valabilitate a unui atestat european individual de competențe în materie de securitate cibernetică eliberat în cadrul sistemului de atestare.

(4) Un sistem de atestare europeană individuală a competențelor în materie de securitate cibernetică poate include costul orientativ al unui atestat european individual de competențe în materie de securitate cibernetică.

(5) ENISA asigură o cooperare strânsă cu statele membre pe tot parcursul elaborării sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică.

(6) Modificarea unui sistem european de atestare individuală a competențelor în materie de securitate cibernetică nu afectează autorizația acordată în temeiul articolului 22 alineatul (3) litera (a), care rămâne valabilă pe perioada pentru care este acordată.

Articolul 21
Furnizori de atestate autorizați

(1) Furnizorii de atestate autorizați evaluează dacă persoanele îndeplinesc cerințele unui sistem de atestare europeană individuală a competențelor în materie de securitate cibernetică și, în cazul în care aceste cerințe sunt îndeplinite, eliberează atestate europene individuale de competențe în materie de securitate cibernetică. Furnizorii de atestare pot deține mai multe autorizații, fiecare fiind acordată pentru un sistem european de atestare individuală a competențelor în materie de securitate cibernetică.

(2) ENISA oferă orientări evaluatorilor și asigură formarea obligatorie a acestora în ceea ce privește cerințele și metodele de evaluare incluse în sistemul european de atestare individuală a competențelor în materie de securitate cibernetică, astfel cum se menționează la articolul 20 alineatul (3) litera (b).

(3) Entitățile care doresc să devină furnizori de atestate autorizați sau să își reînnoiască autorizația („solicitanții”) trebuie să depună o cerere la ENISA. Aceștia trebuie să îndeplinească următoarele condiții:

(a) au personalitate juridică;

(b) sunt în măsură să îndeplinească sarcinile prevăzute în prezentul regulament în ceea ce privește atestatele europene individuale de competențe în materie de securitate cibernetică, indiferent dacă evaluarea este efectuată chiar de furnizorul de atestate autorizat sau în numele și sub responsabilitatea acestuia;

(c) dispun de mijloacele necesare pentru a îndeplini în mod corespunzător sarcinile tehnice și administrative legate de sistemul european de atestare individuală a competențelor în materie de securitate cibernetică și au acces la toate echipamentele și instalațiile necesare.

În sensul primului paragraf litera (b), orice subcontractare sau consultare a personalului extern trebuie să fie documentată în mod adecvat, nu trebuie să implice intermediari și trebuie să facă obiectul unui acord scris care vizează, între altele, confidențialitatea și conflictele de interese.

(4) Solicitanții nu trebuie să fie furnizori cu grad ridicat de risc.

(5) Furnizorii de atestate autorizați trebuie să îndeplinească următoarele obligații:

(a) pentru punerea în aplicare a fiecărui sistem european de atestare individuală a competențelor în materie de securitate cibernetică:

(i) au la dispoziție evaluatorii și personalul necesar pentru a-și desfășura activitățile, astfel cum sunt stabilite în cadrul sistemului respectiv, în timp util;

(ii) se asigură că evaluatorii respectă secretul profesional, sunt imparțiali și își desfășoară activitatea în mod independent și cu cel mai înalt grad de integritate profesională;

(iii) dispun de proceduri scrise pentru desfășurarea activităților lor în cadrul sistemului pentru care sunt autorizați.

(b) nu evaluează și nu eliberează atestate europene individuale de competențe în materie de securitate cibernetică propriilor evaluatori;

(c) se asigură, după caz, prin instituirea unor garanții adecvate, că evaluatorii lor își pot desfășura activitatea în mod independent, în special în cazul în care

aceste persoane aparțin propriei structuri sau sunt angajați sau cursanți ai unei astfel de structuri;

(d) nu se implică în nicio activitate care ar putea intra în conflict cu independența judecății sau cu integritatea evaluatorilor lor;

(e) se asigură că, la cererea persoanei, atestatele electronice aferente atestatelor europene individuale de competențe în materie de securitate cibernetică sunt emise ca atestate electronice ale atributelor într-un format care poate fi stocat în portofelele europene pentru identitatea digitală prevăzute în Regulamentul (UE) nr. 910/2014.

(6) Furnizorii de atestate autorizați informează imediat ENISA în cazul în care oricare dintre cerințele enumerate la alineatele (3) și (4) sau obligațiile enumerate la alineatul (5) nu mai sunt îndeplinite sau în cazul în care apare orice îndoială că cerințele sau obligațiile respective nu sunt îndeplinite, inclusiv în ceea ce privește independența evaluatorilor.

(7) Furnizorii de atestate autorizați pot solicita o taxă din partea persoanelor fizice pentru evaluarea și eliberarea atestatelor europene individuale de competențe în materie de securitate cibernetică, ținând seama de costul orientativ al unui atestat european individual de competențe în materie de securitate cibernetică în temeiul articolului 20 alineatul (4) și pus la dispoziția publicului pe un site dedicat, în conformitate cu articolul 23 litera (d).

(8) Solicitanții și furnizorii de atestate autorizați permit ENISA să efectueze evaluări în cadrul procesului de depunere a cererilor sau de menținere a autorizației și partajează toate informațiile relevante pentru a se asigura că cerințele prevăzute la alineatele (3) și (4) sau obligațiile prevăzute la alineatul (5) sunt îndeplinite sau continuă să fie îndeplinite în conformitate cu articolul 22 alineatul (2).

Articolul 22
Examinarea cererilor de obținere a statutului de furnizor de atestate autorizat și menținerea autorizațiilor

(1) Solicitanții plătesc ENISA o taxă pentru examinarea cererii lor. Furnizorii de atestate autorizați plătesc ENISA o taxă pentru menținerea autorizației lor.

(2) ENISA evaluează dacă cerințele prevăzute la articolul 21 alineatele (3) și (4) și obligațiile prevăzute la articolul 21 alineatul (5) sunt îndeplinite sau continuă să fie îndeplinite de solicitanți și de furnizorii de atestate autorizați.

(3) După examinarea unei cereri în raport cu cerințele prevăzute la articolul 21 alineatele (3) și (4), ENISA poate emite una dintre următoarele decizii:

(a) acordarea statutului de furnizor de atestate autorizat solicitantului sau reînnoirea acestuia;

(b) respingerea cererii de obținere a statutului de furnizor de atestate autorizat sau nereînnoirea acestuia;

(c) închiderea prelucrării cererii din cauza lipsei de acțiune din partea solicitantului în urma unei solicitări de informații suplimentare din partea ENISA.

ENISA poate modifica, suspenda sau revoca astfel de decizii pe baza evaluării sale în temeiul articolului 22 alineatul (2) sau în cazul menționat la articolul 21 alineatul (6).

(4) ENISA emite decizia menționată la alineatul (3) în termen de trei luni de la data depunerii unei cereri în conformitate cu articolul 21 alineatul (3). În cazul în care ENISA a cerut solicitantului informațiile suplimentare, ENISA emite decizia menționată la alineatul (3) în termen de o lună de la primirea informațiilor suplimentare.

(5) Decizia menționată la alineatul (3) litera (a) are o durată maximă de trei ani și indică taxa legată de menținerea anuală a autorizației.

(6) ENISA se asigură că activitățile sale legate de dezvoltarea și adoptarea sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică, astfel cum sunt prevăzute la articolul 20, sunt strict separate și desfășurate independent de activitățile de examinare a cererilor și de evaluare prevăzute la alineatele (2) și (3) de la prezentul articol.

Articolul 23
Informarea publicului

ENISA menține și actualizează periodic un site dedicat care oferă informații publice cu privire la:

(a) ECSF, inclusiv cadrul și calendarul de actualizare a acestuia;

(b) sistemele europene de atestare individuală a competențelor în materie de securitate cibernetică, progresele înregistrate de acestea și termenele pentru dezvoltarea lor;

(c) taxele asociate fiecărui sistem european de atestare individuală a competențelor în materie de securitate cibernetică adoptat în temeiul articolului 47 din prezentul regulament;

(d) costul orientativ al unui atestat european individual de competențe în materie de securitate cibernetică în conformitate cu articolul 20 alineatul (4);

(e) lista furnizorilor de atestate autorizați.

Capitolul III
Organizarea ENISA

Articolul 24
Structura administrativă și de conducere a ENISA

Structura administrativă și de conducere a ENISA cuprinde:

(a) un consiliu de administrație, care exercită funcțiile prevăzute la articolul 28;

(b) un comitet executiv, care exercită funcțiile prevăzute la articolul 30;

(c) un director executiv, căruia îi revin responsabilitățile prevăzute la articolul 32;

(d) un director executiv adjunct, căruia îi revin responsabilitățile prevăzute la articolul 34;

(e) un grup consultativ al ENISA;

(f) o comisie pentru soluționarea contestațiilor care exercită funcțiile prevăzute la articolele 39-42.

Secțiunea 1
Consiliul de administrație

Articolul 25
Componența consiliului de administrație

(1) Consiliul de administrație este compus din câte un membru numit de fiecare stat membru și din doi membri numiți de Comisie. Toți membrii au drept de vot.

(2) Fiecare membru al consiliului de administrație are un supleant. Supleanții îi reprezintă pe membri în absența acestora.

(3) Fiecare stat membru numește șeful unei autorități naționale competente desemnate în temeiul articolului 8 alineatul (1) din Directiva (UE) 2022/2555 în calitate de membru al consiliului de administrație. În cazul în care acest lucru se dovedește a nu fi fezabil, statele membre numesc un reprezentant la nivel înalt al unei autorități naționale competente desemnate în temeiul articolului 8 alineatul (1) din Directiva (UE) 2022/2555 în calitate de membru al consiliului de administrație.

(4) Membrii numiți de Comisie și membrii supleanți ai consiliului de administrație sunt numiți pe baza cunoștințelor lor în domeniul securității cibernetice, ținând seama de competențele lor manageriale, administrative și bugetare relevante. Comisia și statele membre, în ceea ce privește supleanții, urmăresc să obțină o reprezentare echilibrată a bărbaților și femeilor în consiliul de administrație și trebuie să facă eforturi pentru a limita rotația acestora pentru a asigura continuitatea activității consiliului de administrație.

(5) Durata mandatului membrilor numiți de statele membre este egală cu durata funcției lor menționate la alineatul (3).

(6) Mandatul supleanților și al membrilor numiți de Comisie este de patru ani. Acest mandat se poate reînnoi.

Articolul 26
Președintele consiliului de administrație

(1) Consiliul de administrație alege un președinte și un vicepreședinte dintre membrii săi cu drept de vot. Președintele și vicepreședintele sunt aleși cu o majoritate de două treimi din membrii consiliului de administrație cu drept de vot.

(2) Vicepreședintele îl înlocuiește în mod automat pe președinte în cazul în care acesta nu își poate îndeplini atribuțiile.

(3) Mandatul președintelui și al vicepreședintelui are o durată de patru ani și poate fi reînnoit o singură dată. Cu toate acestea, dacă pe durata mandatului încetează calitatea acestora de membri ai consiliului de administrație, mandatul respectiv expiră automat la aceeași dată.

Articolul 27
Reuniunile consiliului de administrație

(1) Președintele convoacă reuniunile consiliului de administrație.

(2) Directorul executiv ia parte la reuniunile consiliului de administrație, fără a avea drept de vot.

(3) Consiliul de administrație se reunește în ședință ordinară cel puțin de două ori pe an. În plus, acesta se reunește la inițiativa președintelui, la solicitarea Comisiei sau la solicitarea a cel puțin o treime dintre membrii săi.

(4) Un reprezentant al Centrului european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică instituit prin Regulamentul (UE) 2021/887 este observator permanent, fără drept de vot, la reuniunile consiliului de administrație.

(5) Consiliul de administrație poate invita orice persoană a cărei opinie poate fi de interes să participe la o reuniune sau la o parte a unei reuniuni, în calitate de observator ad-hoc, fără drept de vot și sub rezerva regulamentului de procedură al consiliului de administrație.

(6) Membrii consiliului de administrație și supleanții lor pot să fie asistați în cursul reuniunilor consiliului de administrație de consilieri sau de experți, sub rezerva regulamentului de procedură al consiliului de administrație.

Articolul 28
Funcțiile consiliului de administrație

(1) Consiliul de administrație:

(a) stabilește direcția generală de funcționare a ENISA și se asigură că ENISA funcționează în conformitate cu normele și principiile prevăzute în prezentul regulament; de asemenea, asigură coerența activității ENISA cu activitățile desfășurate de statele membre, precum și la nivelul Uniunii;

(b) adoptă proiectul de document unic de programare al ENISA menționat la articolul 44, înainte de transmiterea acestuia Comisiei spre avizare;

(c) ținând seama de avizul Comisiei, adoptă documentul unic de programare al ENISA în conformitate cu articolul 29 alineatul (2) litera (a);

(d) supraveghează punerea în aplicare a programării multianuale și anuale cuprinse în documentul unic de programare;

(e) adoptă bugetul anual al ENISA în conformitate cu articolul 29 alineatul (2) litera (b) și exercită alte funcții în ceea ce privește bugetul ENISA în conformitate cu capitolul IV;

(f) evaluează și adoptă raportul anual consolidat privind activitățile ENISA, inclusiv conturile și o descriere a modului în care ENISA și-a îndeplinit indicatorii de performanță; prezintă atât raportul anual, cât și evaluarea acestuia, până la data de 1 iulie a anului următor, Parlamentului European, Consiliului, Comisiei și Curții de Conturi Europene; face public raportul anual;

(g) adoptă normele financiare aplicabile ENISA în conformitate cu articolul 50;

(h) adoptă o strategie de combatere a fraudei care să fie proporțională cu riscurile de fraudă, ținând seama de analiza cost-beneficiu a măsurilor care urmează să fie puse în aplicare;

(i) asigură adoptarea de măsuri subsecvente adecvate pentru a da curs constatărilor și recomandărilor care decurg din rapoartele de audit și evaluările interne sau externe, precum și din investigațiile desfășurate de Oficiul European de Luptă Antifraudă („OLAF”) și de Parchetul European („EPPO”);

(j) adoptă regulamentul de procedură, inclusiv norme pentru decizii provizorii privind delegarea unor atribuții specifice în temeiul articolului 30 alineatul (7);

(k) exercită, în conformitate cu alineatul (2) de la prezentul articol, în ceea ce privește personalul ENISA, competențele conferite prin Statutul funcționarilor Uniunii Europene (denumit în continuare „Statutul funcționarilor”) și, respectiv, prin Regimul aplicabil celorlalți agenți ai Uniunii Europene (denumit în continuare „Regimul aplicabil celorlalți agenți”) prevăzute de Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului[73] autorității împuternicite să facă numiri și autorității abilitate să încheie un contract de muncă („competențele de autoritate împuternicită să facă numiri”);

(l) adoptă norme de punere în aplicare a Statutului funcționarilor și Regimului aplicabil celorlalți agenți în conformitate cu articolul 110 alineatul (2) din Statutul funcționarilor;

(m) numește directorul executiv și, în cazul în care decide să creeze funcția de director executiv adjunct, directorul executiv adjunct și, după caz, prelungește mandatul acestora sau îi demite din funcție în conformitate cu articolul 31;

(n) numește un contabil, căruia i se aplică Statutul funcționarilor și Regimul aplicabil celorlalți agenți și care este independent în îndeplinirea îndatoririlor sale;

(o) ia toate deciziile privind instituirea structurilor interne ale ENISA și, dacă este necesar, privind modificarea acestora, luând în considerare nevoile activității agenției și având în vedere buna gestiune bugetară;

(p) autorizează încheierea acordurilor de lucru în ceea ce privește articolul 68;

(q) autorizează încheierea acordurilor de lucru în conformitate cu articolul 70;

(r) numește și revocă membrii comisiei pentru soluționarea contestațiilor în conformitate cu articolul 29 alineatul (2) litera (d);

(s) adoptă norme de prevenire și de gestionare a conflictelor de interese în ceea ce privește membrii comisiei pentru soluționarea contestațiilor.

(2) În conformitate cu articolul 110 alineatul (2) din Statutul funcționarilor, consiliul de administrație adoptă o decizie în temeiul articolului 2 alineatul (1) din Statutul funcționarilor și al articolului 6 din Regimul aplicabil celorlalți agenți, prin care competențele relevante de autoritate împuternicită să facă numiri îi sunt delegate directorului executiv și în care sunt definite condițiile în care această delegare de competențe poate fi suspendată. Directorul executiv poate să subdelege aceste competențe.

(3) În cazul în care apar împrejurări excepționale care impun acest lucru, consiliul de administrație poate adopta o decizie pentru a suspenda temporar delegarea competențelor de autoritate împuternicită să facă numiri către directorul executiv și delegarea competențelor subdelegate de către directorul executiv și să le exercite el însuși sau să le delege unuia dintre membrii săi ori unui alt membru al personalului decât directorul executiv.

[73] JO L 56, 4.3.1968, p. 1, ELI: http://data.europa.eu/eli/reg/1968/259(1)/oj.

Articolul 29
Regulile de vot ale consiliului de administrație

(1) Consiliul de administrație își adoptă propriile decizii cu majoritatea absolută a membrilor săi cu drept de vot, cu excepția cazului în care prezentul regulament prevede altfel.

(2) O majoritate de două treimi din membrii cu drept de vot ai consiliului de administrație este necesară pentru:

(a) adoptarea documentului unic de programare menționat la articolul 28 alineatul (1) litera (c);

(b) adoptarea bugetului anual menționat la articolul 28 alineatul (1) litera (e);

(c) numirea, prelungirea mandatului sau demiterea directorului executiv și a directorului executiv adjunct, astfel cum se menționează la articolele 31 și 33;

(d) numirea și revocarea membrilor comisiei pentru soluționarea contestațiilor, astfel cum se menționează la articolul 36.

(3) Deciziile privind aspecte legate de buget sau de resursele umane, în special aspectele menționate la articolul 28 alineatul (1) literele (c), (e), (f), (g), (h), (i), (k), (l), (m), (n), se adoptă numai dacă reprezentanții Comisiei au votat favorabil. În scopul adoptării deciziilor menționate la articolul 28 alineatul (1) litera (c) privind documentul unic de programare al ENISA, un vot pozitiv al reprezentantului Comisiei este necesar numai pentru elementele deciziei care nu au legătură cu programul de lucru anual și multianual al ENISA.

(4) Fiecare membru cu drept de vot dispune de un vot. În absența unui membru cu drept de vot, dreptul său de vot poate fi exercitat de supleantul său.

(5) Președintele consiliului de administrație participă la vot.

(6) Directorul executiv nu participă la vot.

(7) Regulamentul de procedură al consiliului de administrație stabilește în mod detaliat modalitățile de vot, în special condițiile în care un membru poate acționa în numele altui membru.

Secțiunea 2
Comitetul executiv

Articolul 30
Comitetul executiv

(1) Consiliul de administrație este asistat de un comitet executiv.

(2) Comitetul executiv:

(a) pregătește deciziile care urmează să fie adoptate de consiliul de administrație;

(b) împreună cu consiliul de administrație, se asigură că se dă curs în mod adecvat constatărilor și recomandărilor care decurg din evaluările și rapoartele de audit interne sau externe, precum și din investigațiile efectuate de OLAF și de EPPO.

(c) fără a aduce atingere responsabilităților directorului executiv, astfel cum se prevede la articolul 32, îi acordă asistență și consiliere directorului executiv în punerea în aplicare a deciziilor consiliului de administrație, pentru a consolida supravegherea gestionării administrative și bugetare.

(3) Comitetul executiv este format din președintele consiliului de administrație, un reprezentant al Comisiei în cadrul consiliului de administrație și trei alți membri numiți de consiliul de administrație din rândul membrilor săi cu drept de vot. Președintele consiliului de administrație este, de asemenea, președintele comitetului executiv. Numirile membrilor comitetului executiv urmăresc asigurarea unei reprezentări echilibrate din perspectiva genului în comitetul executiv. Directorul executiv ia parte la reuniunile comitetului executiv, fără drept de vot.

(4) Durata mandatului membrilor comitetului executiv este de patru ani. Acest mandat se poate reînnoi. Mandatul membrilor comitetului executiv se încheie atunci când încetează mandatul de membru al consiliului de administrație.

(5) Comitetul executiv se reunește în cel puțin o ședință ordinară la fiecare trei luni. În plus, acesta se reunește la inițiativa președintelui său sau la cererea membrilor săi.

(6) Consiliul de administrație stabilește regulamentul de procedură al comitetului executiv.

(7) Atunci când este necesar din motive de urgență, comitetul executiv poate lua anumite decizii provizorii în numele consiliului de administrație, îndeosebi cu privire la aspecte legate de gestionarea administrativă, inclusiv la suspendarea delegării competențelor de autoritate împuternicită să facă numiri, precum și cu privire la aspecte bugetare. Astfel de decizii provizorii se notifică consiliului de administrație fără întârzieri nejustificate. Consiliul de administrație decide dacă aprobă sau respinge decizia provizorie în termen de cel mult trei luni de la luarea deciziei respective. Comitetul executiv nu ia decizii în numele consiliului de administrație care necesită pentru aprobare o majoritate de două treimi din membrii cu drept de vot ai consiliului de administrație.

Secțiunea 3
Directorul executiv

Articolul 31
Numirea, revocarea și prelungirea mandatului

(1) Directorul executiv este numit de consiliul de administrație pe baza meritelor și a competențelor, dintr-o listă de candidați propusă de Comisie, în urma unei proceduri de selecție deschise și transparente.

(2) Înainte de a fi numit în funcție, candidatul selectat de consiliul de administrație este invitat să facă o declarație în fața comisiei competente a Parlamentului European și să răspundă întrebărilor adresate de membrii acesteia.

(3) Directorul executiv este angajat ca agent temporar al ENISA în temeiul articolului 2 litera (a) din Regimul aplicabil celorlalți agenți.

(4) La încheierea contractului cu directorul executiv, ENISA este reprezentată de președintele consiliului de administrație.

(5) Mandatul directorului executiv are o durată de cinci ani. În timp util înainte de sfârșitul acestei perioade, Comisia efectuează o evaluare care ia în considerare evaluarea performanțelor directorului executiv, precum și sarcinile și provocările viitoare ale ENISA.

(6) La propunerea Comisiei, care ține cont de evaluarea menționată la alineatul (5), consiliul de administrație poate prelungi mandatul directorului executiv o singură dată, cu cel mult cinci ani.

(7) Un director executiv al cărui mandat a fost prelungit nu mai poate participa la o altă procedură de selecție pentru același post după încheierea perioadei totale a mandatului său.

(8) Consiliul de administrație informează Parlamentul European în legătură cu intenția sa de a prelungi mandatul directorului executiv în conformitate cu alineatul (6). În cursul perioadei de trei luni care precedă prelungirea mandatului său, directorul executiv, dacă este invitat, face o declarație în fața comisiei relevante a Parlamentului European și răspunde întrebărilor deputaților.

(9) Directorul executiv poate fi demis din funcție numai printr-o decizie a consiliului de administrație, la propunerea Comisiei.

Articolul 32
Atribuțiile și responsabilitățile directorului executiv

(1) Directorul executiv gestionează ENISA și răspunde în fața consiliului de administrație.

(2) Directorul executiv își îndeplinește sarcinile în mod independent, fără a solicita sau primi instrucțiuni de la vreun guvern sau alt organism.

(3) Directorul executiv prezintă Parlamentului European, atunci când este invitat să facă acest lucru, un raport privind modul în care și-a îndeplinit sarcinile. Consiliul îi poate cere directorului executiv să prezinte un raport referitor la modul în care și-a îndeplinit sarcinile.

(4) Directorul executiv este reprezentantul legal al ENISA.

(5) Directorul executiv răspunde de punerea în aplicare a atribuțiilor acordate ENISA în temeiul prezentului regulament. În special, directorul executiv:

(a) asigură administrarea curentă a ENISA;

(b) pune în aplicare deciziile adoptate de consiliul de administrație;

(c) asigură respectarea normelor financiare ale ENISA;

(d) elaborează proiectul de document unic de programare și îl transmite spre aprobare consiliului de administrație înainte de a-l prezenta Comisiei în vederea obținerii unui aviz;

(e) pune în aplicare documentul unic de programare și raportează consiliului de administrație cu privire la punerea sa în aplicare;

(f) elaborează raportul anual de activitate consolidat al ENISA, inclusiv punerea în aplicare a programului anual de activitate al ENISA, și îl prezintă consiliului de administrație spre evaluare și adoptare;

(g) elaborează un plan de acțiune care dă curs concluziilor evaluărilor retrospective ale ENISA, astfel cum se menționează la articolul 121, și prezintă Comisiei, o dată la doi ani, un raport privind progresele înregistrate;

(h) elaborează un plan de acțiune care dă curs concluziilor rapoartelor și evaluărilor de audit interne sau externe și ale investigațiilor OLAF și EPPO și

raportează de două ori pe an Comisiei și periodic consiliului de administrație cu privire la progresele înregistrate;

(i) elaborează proiectul de norme financiare aplicabile ENISA, astfel cum se menționează la articolul 50;

(j) întocmește proiectul de situație a estimărilor de venituri și cheltuieli ale ENISA și execută bugetului acesteia;

(k) protejează interesele financiare ale Uniunii prin aplicarea de măsuri de prevenire a fraudei, a corupției și a oricăror alte activități ilegale, fără a aduce atingere competențelor de investigare ale OLAF și EPPO, prin efectuarea de controale eficace și, în cazul constatării unor nereguli, prin recuperarea sumelor plătite în mod necuvenit și, după caz, prin aplicarea unor sancțiuni administrative eficace, proporționale și disuasive și a unor sancțiuni financiare;

(l) elaborează o strategie antifraudă, o strategie privind sporirea eficienței și realizarea de sinergii, o strategie privind cooperarea cu țările terțe sau cu organizațiile internaționale și o strategie privind gestionarea organizațională și sistemele de control intern pentru ENISA și le prezintă consiliului de administrație spre aprobare;

(m) stabilește și menține contactul cu comunitatea de afaceri și cu organizațiile consumatorilor, în vederea asigurării unui dialog periodic cu părțile interesate relevante;

(n) face schimb periodic de opinii și de informații cu entitățile relevante ale Uniunii cu privire la activitățile lor legate de securitatea cibernetică pentru a asigura coerența punerii în aplicare a politicii Uniunii în acest domeniu;

(o) promovează diversitatea și echilibrul de gen în recrutarea personalului ENISA;

(p) adoptă sisteme europene de atestare individuală a competențelor în materie de securitate cibernetică, astfel cum se menționează la articolul 20 alineatul (1);

(q) adoptă decizii cu privire la solicitanții care doresc să devină furnizori de atestate autorizați sau să își reînnoiască autorizația, astfel cum se menționează la articolul 22 alineatul (3);

(r) îndeplinește alte atribuții care îi sunt încredințate directorului executiv prin prezentul regulament.

(6) După caz, în limitele obiectivelor și atribuțiilor ENISA, directorul executiv poate înființa grupuri de lucru ad-hoc compuse din experți, inclusiv experți din rândul autorităților competente ale statelor membre. Directorul executiv informează în prealabil consiliul de administrație cu privire la acest aspect. Procedurile referitoare în special la componența grupurilor de lucru, la numirea experților acestora de către directorul executiv și la funcționarea lor sunt prevăzute în regulamentul intern de funcționare al ENISA.

(7) Dacă este necesar, în scopul îndeplinirii atribuțiilor ENISA în mod eficient și eficace și pe baza unei analize cost-beneficiu adecvate, directorul executiv poate decide înființarea unuia sau mai multor birouri locale într-unul sau mai multe state membre. Înainte de a decide să înființeze un birou local, directorul executiv cere opinia statului membru sau a statelor membre în cauză, inclusiv a statului membru în care este situat sediul ENISA, și obține acordul prealabil al Comisiei și al consiliului de administrație. În cazurile de dezacord în cursul procesului de consultare între

directorul executiv și statele membre în cauză, chestiunea este supusă Consiliului spre dezbatere. Numărul total al personalului din toate birourile locale este păstrat la minimum și nu depășește 40 % din numărul total al personalului ENISA care se află în statul membru în care este situat sediul ENISA. Numărul personalului din fiecare birou local nu depășește 10 % din numărul total al personalului ENISA care se află în statul membru în care este situat sediul ENISA.

(8) Decizia de înființare a unui birou local precizează domeniul de aplicare al activităților care urmează să fie efectuate în cadrul respectivului birou local, astfel încât să se evite costurile inutile și dublarea funcțiilor administrative ale ENISA.

Secțiunea 4
Directorul executiv adjunct

Articolul 33
Directorul executiv adjunct

(1) Consiliul de administrație poate decide să creeze o funcție de director executiv adjunct care să îl asiste pe directorul executiv.

(2) În cazul în care consiliul de administrație decide să creeze o funcție de director executiv adjunct, directorului executiv adjunct i se aplică dispozițiile articolului 31 în consecință.

Articolul 34
Sarcinile și responsabilitățile directorului executiv adjunct

Directorul executiv adjunct îl asistă pe directorul executiv în gestionarea ENISA și în îndeplinirea sarcinilor menționate la articolul 32. În cazul în care directorul executiv este absent sau se află în imposibilitatea de a-și exercita atribuțiile sau postul este vacant, directorul executiv adjunct îl înlocuiește pe durata absenței sau până la ocuparea postului.

Secțiunea 5
Grupul consultativ al ENISA

Articolul 35
Grupul consultativ al ENISA

(1) Consiliul de administrație, acționând la propunerea directorului executiv, instituie în mod transparent grupul consultativ al ENISA. Grupul consultativ al ENISA este alcătuit din experți recunoscuți care reprezintă părțile interesate relevante, cum ar fi industria securității cibernetice, industria TIC, IMM-urile, entitățile care își desfășoară activitatea în sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555, producătorii de produse cu elemente digitale și administratorii de software cu sursă deschisă în sensul Regulamentului (UE) 2024/2847, organismele de evaluare a conformității notificate în temeiul Cadrului european de certificare a securității cibernetice menționat la articolul 93 și al Regulamentului (UE) 2024/2847, entitățile care își desfășoară activitatea în domeniul mijloacelor de identificare electronică, grupurile de consumatori, experții universitari în domeniul securității cibernetice, organizațiile europene de standardizare, precum și autoritățile de aplicare a legii și autoritățile de supraveghere a protecției datelor. Acești experți recunoscuți

trebuie să fie resortisanți ai statelor membre. Consiliul de administrație depune eforturi pentru a asigura un echilibru adecvat din punct de vedere geografic și al genului, precum și un echilibru între diversele grupuri de părți interesate.

(2) Procedurile privind grupul consultativ al ENISA, în special cele referitoare la componența sa, la propunerea directorului executiv menționată la alineatul (1), la numărul și numirea membrilor săi și la funcționarea grupului consultativ al ENISA, se detaliază în normele interne de funcționare ale ENISA și se fac publice.

(3) Grupul consultativ al ENISA este prezidat de directorul executiv sau de orice persoană numită de acesta de la caz la caz.

(4) Mandatul membrilor grupului consultativ al ENISA este de doi ani și jumătate și poate fi reînnoit o singură dată. Membrii consiliului de administrație nu pot fi membri ai grupului consultativ al ENISA. Experții Comisiei și experții din statele membre au dreptul de a participa la reuniunile grupului consultativ al ENISA și la activitățile acestuia. Directorul executiv poate invita reprezentanți ai altor organisme care nu sunt membri ale grupului consultativ al ENISA să participe la reuniunile grupului consultativ al ENISA și la lucrările acestuia.

(5) Grupul consultativ al ENISA acordă consiliere ENISA în exercitarea atribuțiilor sale, cu excepția aplicării dispozițiilor titlurilor III, IV și V din prezentul regulament. Acesta acordă consiliere în special directorului executiv în ceea ce privește elaborarea unei propuneri de program anual de activitate al ENISA și asigurarea comunicării cu părțile interesate relevante referitor la aspecte legate de programul anual de activitate.

(6) Grupul consultativ al ENISA informează periodic consiliul de administrație despre activitățile sale.

(7) ENISA asigură sprijinul logistic necesar grupului consultativ al ENISA și asigură secretariatul pentru reuniunile acestuia.

Secțiunea 6
Comisia pentru soluționare a contestațiilor

Articolul 36
Înființarea și componența comisiei pentru soluționarea contestațiilor

(1) ENISA instituie o comisie pentru soluționarea contestațiilor printr-o decizie a consiliului de administrație.

(2) Comisia pentru soluționarea contestațiilor este alcătuită dintr-un președinte și alți trei membri. Fiecare membru al comisiei pentru soluționarea contestațiilor are un supleant. Supleantul reprezintă membrul în absența acestuia.

(3) Consiliul de administrație numește președintele, ceilalți membri și supleanții acestora de pe o listă de candidați calificați stabilită de Comisie. Lista candidaților calificați este valabilă timp de patru ani. Valabilitatea acestei liste poate fi prelungită de consiliul de administrație cu perioade suplimentare de patru ani, la propunerea Comisiei.

(4) În cazul în care comisia pentru soluționarea contestațiilor consideră că natura cauzei o impune, aceasta poate solicita consiliului de administrație să numească până la doi alți membri și supleanți ai acestora de pe lista menționată la alineatul (3).

(5) Comisia pentru soluționarea contestațiilor își adoptă propriul regulament de procedură și îl face public.

Articolul 37
Membrii comisiei pentru soluționarea contestațiilor

(1) Mandatul membrilor și al supleanților comisiei pentru soluționarea contestațiilor este de patru ani. Mandatul acestora poate fi reînnoit de către consiliul de administrație pentru perioade suplimentare de patru ani, la propunerea Comisiei.

(2) Membrii comisiei pentru soluționarea contestațiilor sunt independenți și nu îndeplinesc alte atribuții în cadrul ENISA. În procesul de luare a deciziilor, aceștia nu solicită și nu acceptă instrucțiuni de la niciun guvern, de la niciun alt organism și de la nicio entitate privată.

(3) Membrii comisiei pentru soluționarea contestațiilor nu sunt revocați din funcție sau de pe lista candidaților calificați pe durata mandatului lor, cu excepția cazului în care există motive întemeiate pentru o astfel de revocare, iar consiliul de administrație ia o decizie în acest sens, la propunerea Comisiei.

Articolul 38
Excludere și obiecții

(1) Membrii comisiei pentru soluționarea contestațiilor nu iau parte la nicio procedură de soluționare a contestațiilor în cazul în care au un interes personal în procedură, dacă au fost anterior reprezentanții uneia dintre părțile la procedură sau dacă au participat la adoptarea deciziei contestate.

(2) Dacă, pentru unul dintre motivele menționate la alineatul (1) sau pentru orice alt motiv, un membru al unei comisii pentru soluționarea contestațiilor consideră că nu trebuie să participe la procedura de soluționare a contestațiilor, acesta informează comisia pentru soluționarea contestațiilor în mod corespunzător.

(3) O parte la procedura de soluționare a unei contestații poate recuza orice membru al comisiei pentru soluționarea contestațiilor pe baza oricăruia dintre motivele enumerate la alineatul (1) sau în cazul în care membrul respectiv este suspectat de părtinire. O recuzare nu se poate admite dacă, deși a luat cunoștință de un motiv de recuzare, partea implicată în procedura de soluționare a unei contestații a angajat o etapă procedurală. Recuzarea nu se poate fonda în niciun caz pe cetățenia membrilor comisiei pentru soluționarea contestațiilor.

(4) Comisia pentru soluționarea contestațiilor hotărăște măsurile care trebuie luate în cazurile specificate la alineatele (2) și (3), fără participarea membrului în cauză. În scopul luării acestei decizii, membrul în cauză este înlocuit în cadrul comisiei pentru soluționarea contestațiilor de către supleantul său.

Articolul 39
Contestarea deciziilor și a abținerilor de a acționa

(1) Comisia pentru soluționarea contestațiilor poate fi sesizată cu o contestație împotriva:

(a) deciziilor adoptate de ENISA în temeiul articolului 22 alineatul (3);

(b) nerespectării de către ENISA a termenelor aplicabile prevăzute la articolul 22 alineatul (4).

(2) O contestație formulată în temeiul alineatului (1) face obiectul unei revizuiri preliminare în conformitate cu articolul 41 înainte de a fi supusă examinării comisiei pentru soluționarea contestațiilor.

(3) O contestație formulată în temeiul alineatului (1) nu are efect suspensiv.

Articolul 40
Persoane care au dreptul de a introduce o contestație, termene și demersuri

(1) Solicitanții în sensul articolului 21 alineatul (3) pot introduce o contestație împotriva

(a) unei decizii a ENISA care le este adresată, în temeiul articolului 22 alineatul (3);

(b) nerespectării de către ENISA a obligației de a acționa în ceea ce privește o cerere depusă de aceștia la ENISA în termenele aplicabile prevăzute la articolul 22 alineatul (4).

(2) În cazul menționat la alineatul (1) litera (a), contestația, împreună cu expunerea de motive a acesteia, se depune în scris, în conformitate cu regulamentul de procedură menționat la articolul 36 alineatul (5), în termen de două luni de la notificarea deciziei către solicitantul în cauză sau, în absența acesteia, de la data la care solicitantul a luat cunoștință de decizie.

(3) În cazul menționat la alineatul (1) litera (b), contestația se introduce în scris la ENISA, în conformitate cu regulamentul de procedură menționat la articolul 36 alineatul (5), în termen de două luni de la data expirării termenului prevăzut la articolul 22 alineatul (4).

Articolul 41
Revizuire preliminară

(1) Dacă ENISA consideră contestația admisibilă și bine întemeiată, aceasta revine asupra deciziei sau abținerii de a acționa menționate la articolul 40 alineatul (1).

(2) În cazul în care ENISA nu revine asupra deciziei în termen de o lună de la primirea contestației, aceasta decide imediat dacă suspendă aplicarea deciziei sale și înaintează contestația comisiei pentru soluționarea contestațiilor.

Articolul 42
Examinarea deciziilor privind contestațiile

(1) Comisia pentru soluționarea contestațiilor decide, în termen de trei luni de la data introducerii contestației, dacă admite sau respinge contestația respectivă. Atunci când examinează o contestație, comisia pentru soluționarea contestațiilor acționează în termenele stabilite în regulamentul său de procedură. Comisia pentru soluționarea contestațiilor invită părțile la procedura de contestare, ori de câte ori este necesar, să prezinte, în termenele stabilite, observații cu privire la notificările făcute de comisia pentru soluționarea contestațiilor sau la comunicările altor părți la procedura de contestare. Părțile la procedurile de contestație au dreptul să își prezinte oral argumentele.

(2) În cazul în care comisia pentru soluționarea contestațiilor constată că motivele de introducere a unei contestații sunt întemeiate, aceasta înaintează cazul către ENISA. ENISA ia decizia finală în conformitate cu constatările comisiei pentru soluționarea contestațiilor și furnizează o expunere de motive aferentă deciziei respective. ENISA informează în consecință părțile la procedura de contestare.

Articolul 43
Acțiuni în fața Curții de Justiție a Uniunii Europene

(1) Acțiunile în anulare împotriva deciziilor ENISA adoptate în temeiul articolului 22 alineatul (3) sau acțiunile în constatarea abținerii de a acționa în termenele aplicabile în temeiul articolului 22 alineatul (4) pot fi introduse în fața Curții de Justiție a Uniunii Europene, după epuizarea procedurii de soluționare a contestațiilor în cadrul ENISA prevăzute la articolele 39-42 sau în cazul abținerii de a acționa în termenul aplicabil în temeiul articolului 41 alineatul (2).

(2) ENISA ia toate măsurile necesare pentru a aduce la îndeplinire hotărârea Curții de Justiție a Uniunii Europene.

Secțiunea 7
Operațiuni

Articolul 44
Documentul unic de programare

(1) ENISA își desfășoară activitatea în conformitate cu documentul său unic de programare care conține programul său de lucru anual și multianual și care include toate activitățile sale planificate.

(2) În fiecare an, directorul executiv elaborează un proiect de document unic de programare, astfel cum se menționează la alineatul (1), cu planificarea corespunzătoare a resurselor financiare și umane în conformitate cu articolul 32 din Regulamentul delegat (UE) 2019/715 al Comisiei[74] și luând în considerare orientările stabilite de Comisie.

(3) Până la data de 30 noiembrie a fiecărui an, consiliul de administrație adoptă documentul unic de programare menționat la alineatul (1), ținând seama de avizul Comisiei menționat la articolul 32 alineatul (7) din Regulamentul delegat (UE) 2019/715. În cazul în care consiliul de administrație decide să nu ia în considerare vreun element din avizul Comisiei, furnizează o justificare detaliată a deciziei respective. Până la data de 31 ianuarie a anului următor, consiliul de administrație transmite documentul unic de programare Parlamentului European, Consiliului și Comisiei, precum și orice versiune actualizată ulterior a documentului respectiv.

(4) Documentul unic de programare se definitivează după adoptarea definitivă a bugetului general al Uniunii și, dacă este necesar, se ajustează în mod corespunzător.

---

[74] Regulamentul delegat (UE) 2019/715 al Comisiei din 18 decembrie 2018 privind regulamentul financiar cadru pentru organele instituite în temeiul TFUE și al Tratatului Euratom și menționate la articolul 70 din Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului (JO L 122, 10.5.2019, p. 1, ELI: http://data.europa.eu/eli/reg_del/2019/715/oj).

(5) Programul anual de lucru cuprinde obiective detaliate și rezultate preconizate, inclusiv indicatori de performanță. Acesta cuprinde, de asemenea, o descriere a acțiunilor care urmează să fie finanțate și o indicație a resurselor financiare și umane alocate fiecărei acțiuni, în conformitate cu principiile întocmirii bugetului și ale gestionării pe activități. Programul anual de activitate concordă cu programul multianual de activitate menționat la alineatul (7). Aceasta indică în mod clar sarcinile care au fost adăugate, modificate sau eliminate în comparație cu exercițiul financiar precedent.

(6) Consiliul de administrație modifică programul anual de activitate adoptat atunci când o nouă atribuție este încredințată ENISA. Orice modificare substanțială a programului anual de activitate se adoptă prin aceeași procedură ca cea utilizată în cazul programului inițial. Consiliul de administrație poate delega directorului executiv competența de a aduce modificări minore programului anual de lucru.

(7) Programul multianual de activitate stabilește programarea strategică globală, inclusiv obiectivele, rezultatele preconizate și indicatorii de performanță. De asemenea, acesta stabilește programarea resurselor, inclusiv bugetul multianual și personalul.

(8) Programarea resurselor se actualizează în fiecare an. Programarea strategică se actualizează după caz, în special pentru a ține seama de rezultatul evaluării menționate la articolul 120.

CAPITOLUL IV
Întocmirea și structura bugetului ENISA

Articolul 45
Întocmirea bugetului ENISA

(1) În fiecare an, directorul executiv elaborează un proiect estimativ provizoriu al veniturilor și cheltuielilor ENISA pentru exercițiul financiar următor, care conține planul de personal, și îl transmite consiliului de administrație.

(2) Proiectul estimativ provizoriu se bazează pe obiectivele și rezultatele preconizate ale programului anual de lucru și ține cont de resursele financiare necesare pentru atingerea acestor obiective și rezultate preconizate, în conformitate cu principiul bunei gestiuni financiare și al performanței.

(3) Pe baza proiectului estimativ provizoriu, consiliul de administrație adoptă un proiect de buget estimativ al veniturilor și cheltuielilor ENISA pentru exercițiul financiar următor și îl transmite Comisiei până la data de 31 ianuarie a fiecărui an.

(4) Comisia transmite proiectul de estimare autorității bugetare, împreună cu proiectul de buget general al Uniunii. Proiectul de buget estimativ este, de asemenea, pus la dispoziția ENISA.

(5) Pe baza acestui proiect de estimare, Comisia înscrie în proiectul de buget general al Uniunii Europene estimările pe care le consideră necesare pentru schema de personal și valoarea contribuției care trebuie alocată din bugetul general al Uniunii și îl înaintează autorității bugetare în conformitate cu articolele 313 și 314 din TFUE.

(6) Autoritatea bugetară autorizează creditele pentru contribuția de la bugetul general al Uniunii acordată ENISA.

(7) Autoritatea bugetară adoptă planul de personal al ENISA.

(8) Consiliul de administrație adoptă bugetul ENISA. Acesta devine definitiv după adoptarea definitivă a bugetului general al Uniunii și, dacă este necesar, este ajustat în consecință.

(9) În cazul oricărui proiect imobiliar care poate avea implicații semnificative asupra bugetului ENISA, se aplică dispozițiile Regulamentului delegat (UE) 2019/715.

Articolul 46
Structura bugetului ENISA

(1) Se elaborează și se înscriu în bugetul ENISA estimări ale tuturor veniturilor și cheltuielilor ENISA pentru fiecare exercițiu financiar. Exercițiul financiar corespunde anului calendaristic.

(2) Bugetul ENISA trebuie să fie echilibrat în ceea ce privește veniturile și cheltuielile.

(3) Fără a aduce atingere altor resurse, veniturile ENISA sunt alcătuite astfel:

(a) dintr-o contribuție din partea Uniunii, înscrisă în bugetul general al Uniunii;

(b) din venituri alocate unor cheltuieli specifice în conformitate cu normele sale financiare menționate la articolul 50;

(c) dintr-o finanțare din partea Uniunii sub forma unor acorduri de contribuție sau de granturi ad-hoc, în conformitate cu normele financiare ale ENISA menționate la articolul 50 și cu dispozițiile instrumentelor relevante care sprijină politicile Uniunii;

(d) din taxele percepute de la solicitanți pentru activitățile legate de sistemele europene de atestare individuală a competențelor în materie de securitate cibernetică menționate la articolul 22 alineatul (1);

(e) din taxele percepute de la organismele de evaluare a conformității pentru participarea la un sistem european de certificare a securității cibernetice menționat la articolul 47 alineatul (2) și pentru eliberarea certificatelor europene de securitate cibernetică în cadrul unui astfel de sistem;

(f) din taxele percepute de la autoritățile publice sau organismele private pentru instrumentele de testare, astfel cum se menționează la articolul 47 alineatul (3);

(g) din orice contribuție din partea țărilor terțe care participă la activitatea ENISA, astfel cum se prevede la articolul 70 alineatul (4);

(h) din orice contribuție voluntară din partea statelor membre, în bani sau în natură.

(4) Statele membre care furnizează contribuții voluntare, astfel cum se menționează la alineatul (3) litera (g), nu revendică niciun drept sau serviciu specific ca urmare a acestui fapt.

(5) Cheltuielile ENISA includ cheltuielile cu personalul, cheltuielile administrative și de infrastructură, precum și cheltuielile de funcționare.

Articolul 47
Taxe

(1) În legătură cu fiecare activitate a sistemului european de atestare menționat la articolul 22 alineatul (1), se percep următoarele taxe solicitanților în sensul

articolului 21 alineatul (3) sau furnizorilor de atestate autorizați pentru a contribui la acoperirea costurilor totale ale activităților desfășurate de ENISA:

(a) eliberarea autorizațiilor în urma examinării cerințelor prevăzute la articolul 21 alineatele (3) și (4), inclusiv efectuarea de evaluări;

(b) menținerea anuală a autorizației;

(c) reînnoirea autorizațiilor pentru furnizorii de atestate europene individuale de competențe în materie de securitate cibernetică, inclusiv efectuarea de evaluări.

(2) În ceea ce privește certificarea, se percep următoarele taxe organismelor de evaluare a conformității pentru întreținerea sistemelor europene de certificare a securității cibernetice în temeiul cărora sunt eliberate certificatele europene de securitate cibernetică, în special:

(a) o taxă anuală pentru participarea la un sistem european de certificare a securității cibernetice;

(b) o taxă pentru eliberarea de certificate europene de securitate cibernetică în cadrul sistemelor europene de certificare a securității cibernetice.

Taxele menționate la litera (b) se percep atunci când organismul de evaluare a conformității transmite ENISA certificatele europene de securitate cibernetică în vederea publicării pe site-ul său în temeiul articolului 79.

(3) În ceea ce privește instrumentele de testare menționate la articolul 15 alineatul (1), se percepe o taxă de la orice autoritate publică sau organism privat pentru utilizarea acestora.

(4) Taxele se exprimă și se plătesc în euro.

(5) Comisia adoptă acte de punere în aplicare prin care stabilește norme detaliate referitoare la stabilirea taxelor care urmează să fie percepute de ENISA, specificând în special costurile estimate care pot fi atribuite fiecăruia dintre aspectele pentru care se percep taxe în temeiul alineatelor (1), (2) și (3) și cuantumurile individuale ale taxelor percepute, precum și modalitățile și condițiile în care ar trebui plătite taxele. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2). Comisia consultă ENISA atunci când elaborează respectivele proiecte de acte de punere în aplicare.

(6) Taxele stabilite prin actele de punere în aplicare menționate la alineatul (5) trebuie să fie stabilite în prealabil pentru a fi proporționale cu costurile estimate ale activităților efectuate sau ale serviciilor furnizate, astfel cum sunt determinate într-un mod eficient din punctul de vedere al costurilor, și sunt suficiente pentru a acoperi costurile respective. Toate cheltuielile ENISA atribuite personalului implicat în activitățile menționate la alineatele (1), (2) și (3) se reflectă în costurile care trebuie acoperite. Taxele trebuie stabilite la un nivel care să permită evitarea unui deficit sau a unei acumulări semnificative de excedent bugetar al ENISA. Excedentele bugetare generate de taxe se reportează pentru a finanța activitățile ENISA, în special activitățile viitoare legate de taxe, sau pentru a compensa pierderile suferite. În cazul în care un sold pozitiv semnificativ în buget, rezultat din activitățile acoperite de taxe, devine recurent sau în cazul în care un sold negativ semnificativ rezultă din furnizarea serviciilor acoperite de taxe, Comisia modifică actele de punere în aplicare menționate la alineatul (5) pentru a revizui metoda de calculare a taxelor în conformitate cu articolul 118 alineatul (2).

Cuantumul taxelor pentru sarcinile menționate la alineatul (1) se stabilește la un nivel care să asigure faptul că veniturile aferente contribuie suficient la acoperirea costurilor activităților legate de dezvoltarea și întreținerea sistemelor europene de atestare individuală, de prelucrarea cererilor și de eliberarea și reînnoirea autorizațiilor, precum și a costurilor necesare pentru respectivele activități de supraveghere desfășurate de ENISA.

Cuantumul taxelor pentru sarcinile menționate la alineatul (2) se stabilește la un nivel care să asigure faptul că veniturile aferente contribuie suficient la acoperirea costurilor totale ale activităților legate de menținerea sistemelor europene de certificare a securității cibernetice prevăzute la articolul 75.

Cuantumul taxelor pentru sarcinile menționate la alineatul (3) se stabilește la un nivel care să asigure faptul că veniturile aferente contribuie suficient la acoperirea costurilor activităților legate de furnizarea de instrumente de testare, astfel cum se prevede la articolul 15 alineatul (1).

(7) ENISA prezintă un raport privind taxele percepute și impactul acestora asupra bugetului său în cadrul procedurii de prezentare a conturilor prevăzute la articolul 50.

(8) ENISA instituie un set de indicatori pentru a măsura volumul de muncă, eficacitatea și eficiența activităților finanțate prin taxe. ENISA își adaptează planificarea personalului și gestionarea resurselor legate de taxe în mod corespunzător pentru a putea răspunde în mod adecvat unei astfel de cereri și oricăror fluctuații ale veniturilor din taxe. ENISA transmite raportul Comisiei, iar Comisia îl poate utiliza în scopul evaluării menționate la articolul 120 alineatul (1).

Articolul 48
Execuția bugetară a ENISA

(1) Directorul executiv răspunde de execuția bugetului ENISA și acționează în calitate de ordonator de credite.

(2) Auditorul intern al Comisiei exercită asupra ENISA aceleași prerogative ca și asupra serviciilor Comisiei.

(3) În fiecare an, directorul executiv transmite autorității bugetare toate informațiile relevante pentru constatările procedurilor de evaluare.

Articolul 49
Prezentarea conturilor și descărcarea de gestiune

(1) Contabilul ENISA trimite conturile provizorii contabilului Comisiei și Curții de Conturi pentru exercițiul financiar (anul N) până la data de 1 martie a următorului exercițiu financiar (anul N + 1).

(2) Până la data de 1 martie a anului N + 1, contabilul ENISA comunică, de asemenea, informațiile contabile necesare în scopuri de consolidare către contabilul Comisiei, în modul și formatul solicitat de aceasta din urmă.

(3) Până la data de 31 martie a anului N + 1, ENISA trimite raportul privind gestiunea bugetară și financiară pentru anul N Parlamentului European, Consiliului, Comisiei și Curții de Conturi.

(4) După primirea observațiilor formulate de Curtea de Conturi cu privire la conturile provizorii ale ENISA pentru anul N, contabilul ENISA întocmește conturile finale

ale ENISA pe propria răspundere. Directorul executiv le prezintă consiliului de administrație în vederea obținerii unui aviz.

(5) Consiliul de administrație emite un aviz cu privire la conturile finale ale ENISA pentru anul N.

(6) Contabilul ENISA transmite Parlamentului European, Consiliului, Comisiei și Curții de Conturi conturile finale pentru anul N, împreună cu avizul consiliului de administrație, până la data de 1 iulie a anului N + 1.

(7) Până la data de 15 noiembrie a anului N + 1, se publică în *Jurnalul Oficial al Uniunii Europene* un link către paginile web care conțin conturile finale ale ENISA.

(8) Până la data de 30 septembrie a anului N + 1, directorul executiv trimite Curții de Conturi, un răspuns la observațiile cuprinse în raportul anual al acesteia. Directorul executiv trimite de asemenea răspunsul respectiv consiliului de administrație și Comisiei.

(9) Directorul executiv prezintă Parlamentului European, la solicitarea acestuia din urmă, toate informațiile necesare pentru a facilita aplicarea procedurii de descărcare de gestiune pentru anul N, în conformitate cu articolul 267 alineatul (3) din Regulamentul (UE, Euratom) 2024/2509 al Parlamentului European și al Consiliului.

(10) La recomandarea Consiliului, care hotărăște cu majoritate calificată, Parlamentul European acordă directorului executiv, înaintea datei de 15 mai a anului N + 2, descărcarea de gestiune în ceea ce privește execuția bugetului pentru anul N.

Articolul 50
Normele financiare

(1) Normele financiare aplicabile ENISA se adoptă de către consiliul de administrație după consultarea Comisiei. Acestea nu derogă de la dispozițiile Regulamentului delegat (UE) 2019/715, cu excepția cazului în care o astfel de derogare este necesară în mod special pentru funcționarea ENISA, iar Comisia și-a dat acordul prealabil.

(2) ENISA își stabilește și își execută bugetul în conformitate cu normele sale financiare și cu Regulamentul (UE, Euratom) 2024/2509.

Articolul 51
Combaterea fraudei

(1) Pentru a combate frauda, corupția și alte activități ilicite, activităților ENISA li se aplică fără restricție dispozițiile Regulamentului (UE, Euratom) nr. 883/2013 al Parlamentului European și al Consiliului[75].

(2) ENISA aderă la Acordul interinstituțional din 25 mai 1999 dintre Parlamentul European, Consiliul Uniunii Europene și Comisia Comunităților Europene privind investigațiile interne desfășurate de Oficiul European de Luptă Antifraudă (OLAF)[76] în termen de șase luni de la *[OP: a se introduce data exactă, menționată la articolul*

[75] Regulamentul (UE, Euratom) nr. 883/2013 al Parlamentului European și al Consiliului din 11 septembrie 2013 privind investigațiile efectuate de Oficiul European de Luptă Antifraudă (OLAF) și de abrogare a Regulamentului (CE) nr. 1073/1999 al Parlamentului European și al Consiliului și a Regulamentului (Euratom) nr. 1074/1999 al Consiliului (JO L 248, 18.9.2013, p. 1, ELI: http://data.europa.eu/eli/reg/2013/883/oj).

[76] JO L 136, 31.5.1999, p. 15, ELI: http://data.europa.eu/eli/agree_interinstit/1999/531/oj.

127] și adoptă dispozițiile corespunzătoare aplicabile întregului său personal, folosind modelul prevăzut în anexa la acordul respectiv.

(3) Curtea de Conturi are competența de a audita, pe bază de documente și prin controale la fața locului, toți beneficiarii de granturi, contractanții și subcontractanții care au primit fonduri din partea Uniunii acordate de ENISA.

(4) OLAF poate desfășura investigații, inclusiv controale și inspecții la fața locului, pentru a stabili dacă s-a comis o fraudă, un act de corupție sau orice altă activitate ilegală care afectează interesele financiare ale Uniunii în legătură cu un grant sau un contract finanțat de ENISA, în conformitate cu dispozițiile și cu procedurile stabilite în Regulamentul (UE, Euratom) nr. 883/2013 și în Regulamentul (Euratom, CE) nr. 2185/96 al Consiliului[77].

(5) Fără a aduce atingere alineatelor (1)-(4), acordurile de lucru cu țările terțe și cu organizațiile internaționale, contractele, acordurile de grant și deciziile privind granturile luate de ENISA trebuie să conțină prevederi care împuternicesc în mod expres Curtea de Conturi și OLAF să desfășoare astfel de audituri și investigații, conform competențelor care le revin.

(6) În conformitate cu Regulamentul (UE) 2017/1939 al Consiliului, EPPO poate investiga și urmări penal cazuri de fraudă și alte activități ilegale care afectează interesele financiare ale Uniunii, conform dispozițiilor Directivei (UE) 2017/1371 a Parlamentului European și a Consiliului[78].

Articolul 52
Declarația de interese

(1) Membrii consiliului de administrație, directorul executiv, directorul executiv adjunct și funcționarii detașați temporar de statele membre întocmesc, fiecare în parte, o declarație de angajamente și o declarație în care menționează absența sau prezența oricăror interese directe sau indirecte despre care s-ar putea considera că aduc atingere independenței lor. Declarațiile trebuie să fie exacte și complete, se fac anual în scris și se actualizează ori de câte ori este nevoie.

(2) Membrii consiliului de administrație, directorul executiv, directorul executiv adjunct și experții externi care participă la grupurile de lucru ad-hoc declară, fiecare în parte, precis și complet, cel târziu la începutul fiecărei reuniuni, toate interesele care ar putea fi considerate ca aducând atingere independenței lor în ceea ce privește punctele de pe ordinea de zi și se abțin de la participarea la dezbaterile referitoare la punctele respective și de la votul în legătură cu acestea.

(3) ENISA stabilește, în regulamentul său intern de funcționare, modalitățile practice pentru normele referitoare la declarațiile de interese menționate la alineatele (1) și (2).

---

77 Regulamentul (Euratom, CE) nr. 2185/96 al Consiliului din 11 noiembrie 1996 privind controalele și inspecțiile la fața locului efectuate de Comisie în scopul protejării intereselor financiare ale Comunităților Europene împotriva fraudei și a altor abateri (JO L 292, 15.11.1996, p. 2, ELI: http://data.europa.eu/eli/reg/1996/2185/oj).

78 Directiva (UE) 2017/1371 a Parlamentului European și a Consiliului din 5 iulie 2017 privind combaterea fraudelor îndreptate împotriva intereselor financiare ale Uniunii prin mijloace de drept penal (JO L 198, 28.7.2017, p. 29, ELI: http://data.europa.eu/eli/dir/2017/1371/oj).

Articolul 53
Transparență

(1) ENISA își desfășoară activitățile cu un nivel ridicat de transparență și în conformitate cu articolul 55.

(2) ENISA se asigură că publicului și tuturor părților interesate li se furnizează informații adecvate, obiective, fiabile și ușor accesibile, în special în ceea ce privește rezultatele activității sale. De asemenea, aceasta pune la dispoziția publicului declarațiile de interese întocmite în conformitate cu articolul 52.

(3) Consiliul de administrație, pe baza unei propuneri din partea directorului executiv, poate autoriza părțile interesate să participe ca observatori la unele dintre activitățile ENISA.

(4) ENISA stabilește, în regulamentul său intern de funcționare, modalitățile practice de punere în aplicare a normelor privind transparența menționate la alineatele (1) și (2).

Articolul 54
Confidențialitatea în cadrul ENISA

(1) Fără a aduce atingere articolului 55, ENISA nu divulgă terților informațiile pe care le prelucrează sau pe care le primește și pentru care s-a cerut, printr-o solicitare motivată, un tratament confidențial.

(2) Membrii consiliului de administrație, directorul executiv, directorul executiv adjunct, membrii Grupului consultativ al ENISA, experții externi care participă la grupurile de lucru ad-hoc și membrii personalului ENISA, inclusiv funcționarii detașați temporar de statele membre, respectă cerințele de confidențialitate prevăzute la articolul 339 din TFUE, chiar și după încetarea atribuțiilor lor.

(3) ENISA stabilește, în regulamentul său intern de funcționare, modalitățile practice de punere în aplicare a normelor de confidențialitate menționate la alineatele (1) și (2).

Articolul 55
Accesul la documente

(1) Regulamentul (CE) nr. 1049/2001 se aplică documentelor deținute de ENISA.

(2) Consiliul de administrație adoptă modalitățile de punere în aplicare a Regulamentului (CE) nr. 1049/2001.

(3) Deciziile adoptate de ENISA în temeiul articolului 8 din Regulamentul (CE) nr. 1049/2001 pot face obiectul unei plângeri adresate Ombudsmanului European în temeiul articolului 228 din TFUE sau al unei acțiuni înaintate Curții de Justiție a Uniunii Europene în temeiul articolului 263 din TFUE.

CAPITOLUL V
Personalul și ofițerii de legătură

Articolul 56
Dispoziții generale

(1) Personalului ENISA i se aplică Statutul funcționarilor și Regimul aplicabil celorlalți agenți, precum și normele adoptate de comun acord de instituțiile Uniunii pentru

punerea în aplicare a Statutului funcționarilor și a Regimului aplicabil celorlalți agenți.

(2) Personalul ENISA, ofițerii de legătură și experții naționali detașați la ENISA sunt supuși unei proceduri adecvate de autorizare de securitate.

Articolul 57
Privilegii și imunități

Protocolul nr. 7 privind privilegiile și imunitățile Uniunii Europene anexat la TFUE se aplică ENISA și personalului acesteia.

Articolul 58
Ofițerii de legătură

(1) Fiecare stat membru desemnează cel puțin doi ofițeri de legătură din partea unei autorități naționale competente desemnate în temeiul articolului 8 alineatul (1) din Directiva (UE) 2022/2555 în calitate de experți naționali detașați la ENISA pentru a lucra la sediul acesteia sau la biroul său local, în conformitate cu articolul 59 alineatul (2). Comisia poate desemna, de asemenea, un ofițer de legătură.

(2) Ofițerii de legătură contribuie la îndeplinirea sarcinilor ENISA, inclusiv prin facilitarea cooperării operaționale și a schimbului de informații, astfel cum se menționează la articolul 11. Ofițerii de legătură sprijină, de asemenea, ENISA în diseminarea de informații cu privire la activitățile, constatările și recomandările sale către părțile interesate relevante din întreaga Uniune. De asemenea, aceștia îndeplinesc funcția de punct de contact național pentru întrebările din partea statelor lor membre și cele referitoare la statele lor membre, fie răspunzând acestor întrebări în mod direct, fie menținând contactul cu administrațiile lor naționale.

(3) Ofițerii de legătură desemnați de statele lor membre au dreptul de a solicita și de a primi toate informațiile relevante din partea statelor lor membre, astfel cum se prevede în prezentul regulament, respectând pe deplin legislația națională și practicile statului membru, în special în ceea ce privește protecția datelor și confidențialitatea.

Articolul 59
Experții naționali detașați și alte categorii de personal

(1) ENISA poate recurge la experți naționali detașați sau la alte categorii de personal care nu sunt angajate de ENISA, în orice domeniu al activității sale. Acestei categorii de personal nu i se aplică Statutul funcționarilor și Regimul aplicabil celorlalți agenți.

(2) Consiliul de administrație adoptă o decizie de stabilire a normelor aplicabile detașării experților naționali, inclusiv a ofițerilor de legătură, la ENISA.

CAPITOLUL VI
DISPOZIȚII GENERALE PRIVIND ENISA

Articolul 60
Statutul juridic al ENISA

(1) ENISA este un organ al Uniunii cu personalitate juridică.

(2) În fiecare stat membru, ENISA dispune de cea mai extinsă capacitate juridică acordată persoanelor juridice în temeiul dreptului intern al statului membru respectiv. Aceasta poate, în special, să dobândească sau să înstrăineze bunuri mobile și imobile și se poate constitui parte în procedurile judiciare.

(3) ENISA este reprezentată de directorul său executiv.

Articolul 61
Sediul

ENISA își are sediul la Atena, Grecia.

Articolul 62
Acordul privind sediul și condițiile de funcționare

(1) Prevederile necesare referitoare la sediul care urmează să fie pus la dispoziția ENISA în statul membru gazdă și la facilitățile care urmează să fie oferite de statul membru respectiv, precum și normele specifice aplicabile în statul membru gazdă directorului executiv, membrilor consiliului de administrație, personalului ENISA și membrilor familiilor acestora se stabilesc într-un acord privind sediul, încheiat între ENISA și statul membru gazdă după obținerea aprobării consiliului de administrație.

(2) Statul membru care găzduiește ENISA pune la dispoziție cele mai bune condiții posibile pentru a asigura buna funcționare a ENISA, ținând cont de accesibilitatea amplasamentului, existența unor facilități adecvate de educație pentru copiii personalului, un acces corespunzător la piața muncii, la securitate socială și la asistență medicală atât pentru copiii, cât și pentru soții sau soțiile personalului.

Articolul 63
Controlul administrativ

Activitățile ENISA fac obiectul supravegherii de către Ombudsmanul European, în conformitate cu articolul 228 din TFUE.

Articolul 64
Răspunderea ENISA

(1) Răspunderea contractuală a ENISA este reglementată de legea aplicabilă contractului în cauză.

(2) Curtea de Justiție a Uniunii Europene este competentă să se pronunțe în temeiul oricărei clauze compromisorii cuprinse într-un contract încheiat de ENISA.

(3) În materie de răspundere necontractuală, ENISA, repară orice prejudiciu cauzat de personalul său în cursul exercitării atribuțiilor acestuia, în conformitate cu principiile generale comune legislațiilor statelor membre.

(4) Curtea de Justiție a Uniunii Europene este competentă în litigiile privind acordarea de despăgubiri pentru prejudiciile menționate la alineatul (3).

(5) Răspunderea individuală a membrilor personalului ENISA față de ENISA este reglementată de dispozițiile stabilite în Statutul funcționarilor sau în Regimul aplicabil acestora.

Articolul 65
Regimul lingvistic

(1) Regulamentul nr. 1 al Consiliului[79] se aplică ENISA. Statele membre și celelalte organisme desemnate de către statele membre se pot adresa ENISA și pot primi răspunsuri în una dintre limbile oficiale ale instituțiilor Uniunii, la alegerea acestora.

(2) Serviciile de traducere și toate celelalte servicii lingvistice necesare pentru funcționarea ENISA, altele decât serviciile de interpretare, sunt furnizate de Centrul de Traduceri pentru Organismele Uniunii Europene.

Articolul 66
Protecția datelor cu caracter personal

(1) Prelucrarea datelor cu caracter personal de către ENISA face obiectul Regulamentului (UE) 2018/1725.

(2) Consiliul de administrație adoptă normele de punere în aplicare astfel cum se menționează la articolul 45 alineatul (3) din Regulamentul (UE) 2018/1725. Consiliul de administrație poate adopta dispozițiile suplimentare necesare pentru aplicarea de către ENISA a Regulamentului (UE) 2018/1725.

Articolul 67
Norme de securitate privind protecția informațiilor sensibile neclasificate și a informațiilor clasificate

În acord cu Comisia, ENISA adoptă norme de securitate care pun în aplicare principiile de securitate cuprinse în normele de securitate ale Comisiei pentru protecția informațiilor sensibile neclasificate și a IUEC, astfel cum sunt prevăzute în Deciziile (UE, Euratom) 2015/443[80] și (UE, Euratom) 2015/444[81]. Respectivele norme de securitate includ dispoziții privind schimbul, prelucrarea și stocarea unor astfel de informații.

Articolul 68
Cooperarea cu entitățile Uniunii și cu autoritățile naționale

(1) Pentru a asigura coerența, a crea sinergii și a aborda chestiuni de interes comun, ENISA cooperează în chestiuni legate de securitatea cibernetică cu CERT-UE și cu entitățile relevante ale Uniunii, inclusiv cu Europol, cu Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică instituit în temeiul Regulamentului (UE) 2021/887 și cu Comitetul european pentru protecția datelor instituit în temeiul articolului 68 alineatul (1) din Regulamentul (UE) 2016/679.

(2) Cooperarea menționată la alineatul (1) poate fi asigurată prin:

(a) schimbul de know-how și de bune practici;

---

79 Regulamentul nr. 1 de stabilire a regimului lingvistic al Comunității Economice Europene (JO 17, 6.10.1958, p. 385, ELI: http://data.europa.eu/eli/reg/1958/1(1)/oj).

80 Decizia (UE, Euratom) 2015/443 a Comisiei din 13 martie 2015 privind securitatea în cadrul Comisiei (JO L 72, 17.3.2015, p. 41, ELI: http://data.europa.eu/eli/dec/2015/443/oj).

81 Decizia (UE, Euratom) 2015/444 a Comisiei din 13 martie 2015 privind normele de securitate pentru protecția informațiilor UE clasificate (JO L 72, 17.3.2015, p. 53, ELI: http://data.europa.eu/eli/dec/2015/444/oj).

(b) furnizarea de consiliere și emiterea de orientări cu privire la aspecte legate de securitatea cibernetică;

(c) stabilirea modalităților practice pentru executarea unor atribuții specifice, după consultarea Comisiei.

(3) ENISA se angajează într-o cooperare structurată cu CERT-UE, în special în ceea ce privește aspectele legate de consolidarea capacităților, cooperarea operațională și analizele strategice pe termen lung ale amenințărilor cibernetice.

(4) ENISA cooperează și face schimb de informații cu autoritățile relevante de supraveghere a pieței și de supraveghere desemnate în temeiul legislației Uniunii în domeniul securității cibernetice, inclusiv al Regulamentului (UE) 2024/2847.

Articolul 69
Cooperarea cu părțile interesate

(1) În cazul în care acest lucru este necesar pentru atingerea obiectivelor prezentului regulament, ENISA cooperează cu părțile interesate relevante, cum ar fi industria securității cibernetice, industria TIC, IMM-urile, entitățile care își desfășoară activitatea în sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555, producătorii, importatorii sau distribuitorii de produse cu elemente digitale în sensul Regulamentului (UE) 2024/2847, organismele de evaluare a conformității notificate în temeiul cadrului european de certificare a securității cibernetice și al Regulamentului (UE) 2024/2847, entitățile care își desfășoară activitatea în domeniul mijloacelor de identificare electronică, grupurile de consumatori și experții universitari în domeniul securității cibernetice. În acest scop, ENISA poate institui parteneriate public-privat.

(2) În consultare cu Comisia, ENISA sprijină cooperarea dintre organismele de evaluare a conformității notificate în temeiul articolului 93. În special, aceasta poate institui un grup de organisme de evaluare a conformității notificate pentru schimbul de bune practici, creând sinergii cu alte acte legislative relevante ale Uniunii, în special cu Regulamentul (UE) 2024/2847.

Articolul 70
Cooperarea cu țările terțe și cu organizațiile internaționale

(1) În măsura în care este necesar pentru atingerea obiectivelor prezentului regulament, ENISA poate coopera cu autoritățile competente din țări terțe sau cu organizații internaționale sau cu ambele, în conformitate cu prioritățile Uniunii. În acest scop, ENISA poate stabili acorduri de lucru cu autoritățile din țări terțe și cu organizații internaționale, sub rezerva aprobării prealabile a Comisiei. Aceste acorduri de lucru nu creează obligații legale pentru Uniune și pentru statele membre ale acesteia.

(2) Consiliul de administrație adoptă o strategie pentru relațiile cu țările terțe și cu organizațiile internaționale în ceea ce privește aspectele pentru care ENISA este competentă și în conformitate cu prioritățile menționate la alineatul (1). Comisia se asigură că ENISA își desfășoară activitatea în limitele mandatului său și în cadrul instituțional existent prin încheierea de acorduri de lucru adecvate cu directorul agenției.

(3) Pentru a sprijini cooperarea cu țările terțe, în special cu țările candidate la aderarea la Uniune, ENISA își poate furniza expertiza în materie de consolidare a capacităților, în special în următoarele domenii:

(a) evaluarea nivelului de maturitate al capacităților și resurselor în materie de securitate cibernetică;

(b) creșterea și consolidarea forței de muncă din domeniul securității cibernetice, inclusiv prin promovarea ECSF și a sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică și prin furnizarea de activități de învățare și formare;

(c) sprijinirea planificării și a executării exercițiilor de securitate cibernetică.

(4) ENISA este deschisă participării la activitatea ENISA a țărilor terțe care au încheiat acorduri cu Uniunea în acest sens. În temeiul dispozițiilor relevante ale acordurilor încheiate între țări terțe și Uniune, se stabilesc acorduri de lucru, sub rezerva aprobării prealabile de către Comisie, în care se precizează în special natura, amploarea și modul în care aceste țări terțe urmează să participe la activitatea ENISA și care includ dispoziții referitoare la participarea la inițiativele întreprinse de ENISA, la contribuțiile financiare și la personal. În ceea ce privește chestiunile legate de personal, aceste acorduri de lucru respectă, în orice caz, Statutul funcționarilor și Regimul aplicabil celorlalți agenți.

(5) ENISA raportează periodic Consiliului și Comisiei cu privire la punerea în aplicare a acordurilor de lucru menționate la alineatele (1) și (4).

TITLUL III

CADRUL EUROPEAN DE CERTIFICARE A SECURITĂȚII CIBERNETICE

CAPITOLUL I
Obiective, domeniu de aplicare și proceduri

Articolul 71
Obiectivele și domeniul de aplicare al cadrului european de certificare a securității cibernetice

(1) Se instituie cadrul european de certificare a securității cibernetice în vederea creării unei piețe unice digitale pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate și entități. În acest scop, aceasta sporește nivelul de securitate cibernetică în Uniune și permite o abordare armonizată a sistemelor europene de certificare a securității cibernetice, precum și valorificarea certificării pentru a facilita conformitatea cu legislația aplicabilă a Uniunii.

(2) Cadrul european de certificare a securității cibernetice prevede un mecanism de instituire a unor sisteme europene de certificare a securității cibernetice și de atestare a următoarelor elemente:

(a) că produsele TIC, serviciile TIC și procesele TIC care au fost evaluate în conformitate cu sistemele respective sunt conforme cu cerințele de securitate specificate, cu scopul de a proteja disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise ori prelucrate sau funcțiile ori

serviciile oferite de aceste produse, servicii și procese sau accesibile prin intermediul acestora pe întregul lor ciclu de viață.

(b) că serviciile de securitate gestionate care au fost evaluate în conformitate cu astfel de sisteme respectă cerințele de securitate specificate cu scopul de a proteja disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor care sunt accesate, prelucrate, stocate sau transmise în legătură cu furnizarea serviciilor respective și că serviciile respective sunt furnizate în mod continuu de personal care are competența, expertiza și experiența necesare, cu un nivel suficient și adecvat de cunoștințe tehnice relevante și de integritate profesională;

(c) că postura de securitate cibernetică a unei entități care a fost evaluată în conformitate cu astfel de sisteme respectă cerințele de securitate cibernetică specificate.

(3) Certificarea europeană a securității cibernetice este voluntară, cu excepția cazului în care se prevede altfel în dreptul Uniunii sau în dreptul intern.

(4) Un certificat european de securitate cibernetică și o declarație de conformitate UE emise în temeiul cadrului european de certificare a securității cibernetice sunt recunoscute automat în toate statele membre.

Articolul 72
Informarea și consultarea publicului

(1) Cel puțin o dată pe an, Comisia organizează, cu sprijinul ENISA, o Adunare europeană pentru certificarea securității cibernetice, invitând membrii ECCG și alți experți relevanți din statele membre, experți relevanți din entitățile Uniunii și părți interesate relevante să discute prioritățile strategice pentru armonizare în domeniul certificării securității cibernetice.

(2) Comisia menține și actualizează periodic un site dedicat care oferă informații cu privire la următoarele aspecte:

(a) sistemele europene de certificare de securitate cibernetică a căror dezvoltare este solicitată în temeiul articolului 73;

(b) prioritățile strategice pentru armonizarea produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate, a posturii de securitate cibernetică a entităților sau a cerințelor de securitate din legislația Uniunii, inclusiv domeniile potențiale pentru care ar putea fi solicitat un sistem european de certificare a securității cibernetice.

(3) Comisia pune la dispoziția publicului, pe site-ul menționat la alineatul (2) de la prezentul articol, informațiile transmise de ENISA referitoare la cererea sa de a pregăti o propunere de sistem, astfel cum se menționează la articolul 73 și decizia sa de a accepta, de a respinge sau de a întrerupe o propunere de sistem transmisă de ENISA în conformitate cu articolul 74 alineatul (7).

(4) Pe durata elaborării de către ENISA a unei propuneri de sistem în temeiul articolului 74, Parlamentul European și Consiliul pot solicita Comisiei, în calitatea sa de președinte al ECCG, și ENISA să prezinte informații relevante cu privire la proiectul respectivei propuneri de sistem. La cererea Parlamentului European sau a Consiliului, ENISA, de comun acord cu Comisia și fără a aduce atingere articolului 54, poate pune la dispoziția Parlamentului European și a Consiliului

părțile relevante ale proiectului unei propuneri de sistem, într-un mod adecvat nivelului de confidențialitate necesar și, după caz, în mod restrâns.

(5) Parlamentul European și Consiliul pot invita Comisia și ENISA să discute aspecte legate de punerea în aplicare a sistemelor europene de certificare a securității cibernetice pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura de securitate cibernetică a entităților.

Articolul 73

Solicitarea unui sistem european de certificare a securității cibernetice

(1) Comisia poate solicita ENISA să pregătească o propunere de sistem european de certificare a securității cibernetice pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura de securitate cibernetică a entităților.

(2) În cazuri justificate în mod corespunzător, ECCG poate sugera Comisiei să prezinte o solicitare menționată la alineatul (1).

(3) Solicitarea menționată la alineatul (1) detaliază scopul, domeniul de aplicare și modalitățile de îndeplinire a obiectivelor și elementelor de securitate relevante prevăzute la articolele 80 și 81. Solicitarea specifică, de asemenea, planul de dezvoltare a propunerii de sistem european de certificare a securității cibernetice și specificațiile tehnice relevante care trebuie menționate sau definite în sistem.

(4) Atunci când pregătește solicitarea menționată la alineatul (1), Comisia consultă în mod corespunzător ENISA și ECCG și ține seama de opiniile tuturor părților interesate relevante și ale altor entități ale Uniunii, inclusiv, după caz, de cele care sunt relevante în temeiul legislației Uniunii în cadrul căreia un sistem european de certificare a securității cibernetice demonstrează conformitatea și oferă prezumția de conformitate.

Articolul 74

Pregătirea și adoptarea sistemelor europene de certificare a securității cibernetice

(1) În termen de cel mult 12 luni de la primirea unei solicitări din partea Comisiei în temeiul articolului 73, cu excepția cazului în care se prevede altfel în solicitare, ENISA pregătește o propunere de sistem european de certificare a securității cibernetice care îndeplinește cerințele prevăzute la articolele 80 și 81.

(2) Pentru pregătirea fiecărei propuneri de sistem, ENISA instituie un grup de lucru ad-hoc în conformitate cu articolul 32 alineatul (6), cu scopul de a oferi ENISA consultanță de specialitate.

(3) Atunci când pregătește propunerea de sistem, ENISA cooperează îndeaproape cu ECCG. ECCG oferă ENISA asistență și consiliere de specialitate în ceea ce privește pregătirea propunerii de sistem și, după caz, a specificațiilor tehnice justificative.

(4) Atunci când pregătește propunerea de sistem, inclusiv, după caz, specificațiile tehnice justificative, ENISA consultă părțile interesate în timp util prin intermediul unui proces de consultare formal, deschis, transparent și favorabil incluziunii. ENISA cooperează, de asemenea, cu autoritățile publice relevante din statele membre și cu entitățile relevante ale Uniunii pentru a obține consiliere de specialitate din partea acestora în ceea ce privește pregătirea propunerii de sistem și, după caz, a specificațiilor tehnice justificative. Atunci când transmite Comisiei propunerea de

sistem în temeiul alineatului (6), ENISA trebuie să descrie modul în care a respectat prezentul alineat.

(5) Înainte de a transmite Comisiei propunerea de sistem și, după caz, specificațiile tehnice justificative, ENISA solicită membrilor ECCG să furnizeze avize scrise cu privire la propunerea de sistem. Avizele se transmit în termen de cel mult 30 de zile de la data solicitării. ENISA ține seama în cea mai mare măsură de avizele membrilor ECCG. Absența acestor avize nu împiedică ENISA să transmită Comisiei propunerea de sistem.

(6) ENISA transmite Comisiei propunerea de sistem în termen de cel mult 60 de zile de la data solicitării menționate la alineatul (5).

(7) Atunci când primește propunerea de sistem, Comisia evaluează dacă sistemul corespunde solicitării formulate în conformitate cu articolul 73. În termen de 30 de zile de la data transmiterii respectivei propuneri de sistem, Comisia întreprinde una dintre următoarele acțiuni:

(a) acceptă propunerea de sistem;

(b) returnează propunerea de sistem către ENISA în vederea revizuirii, împreună cu o justificare a acestei returnări și cu un termen care să nu depășească 90 de zile, în care ENISA furnizează o propunere de sistem revizuită;

(c) întrerupe propunerea de sistem.

(8) În cazul în care Comisia returnează către ENISA o propunere de sistem în vederea revizuirii în conformitate cu alineatul (7) litera (b), alineatele (4), (5) și (7) se aplică în consecință.

(9) Pe baza propunerii de sistem acceptate pregătite de ENISA, Comisia este împuternicită să adopte acte de punere în aplicare care să prevadă un sistem european de certificare a securității cibernetice pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura de securitate cibernetică a entităților care îndeplinesc cerințele prevăzute la articolele 80 și 81. Acest act de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2).

(10) Comisia poate face trimitere la specificațiile tehnice elaborate de ENISA în actele de punere în aplicare menționate la alineatul (9) de la prezentul articol, în conformitate cu articolele 18 și 77.

(11) Comisia poate specifica condițiile pentru recunoașterea internațională a certificatelor europene de securitate cibernetică în actele de punere în aplicare menționate la alineatul (9) de la prezentul articol, în conformitate cu articolul 87.

Articolul 75

Întreținerea unui sistem european de certificare a securității cibernetice

(1) Fiecare sistem european de certificare a securității cibernetice stabilește o strategie de întreținere. Strategia de întreținere trebuie să prezinte așteptările în ceea ce privește activitățile de întreținere, în special cele legate de standardele sau specificațiile tehnice menționate în sistem și de interacțiunea cu părțile interesate relevante.

(2) În cooperare cu Comisia și cu sprijinul ECCG și al subgrupului său de întreținere relevant, ENISA asigură întreținerea sistemelor europene de certificare a securității cibernetice, inclusiv în vederea unei posibile revizuiri a acestor sisteme de către

Comisie. ENISA cooperează și face schimb de informații cu entitățile și grupurile relevante ale Uniunii în ceea ce privește activitățile de întreținere.

(3) ENISA poate organiza implicarea sectorului privat pentru întreținerea unui sistem sub forma unui grup de lucru ad-hoc în conformitate cu strategia de întreținere menționată la alineatul (1).

(4) Activitățile de întreținere a sistemelor europene de certificare a securității cibernetice includ următoarele:

(a) pregătirea, actualizarea și aprobarea specificațiilor tehnice și a orientărilor pentru a sprijini funcționarea armonizată și uniformă a sistemelor;

(b) identificarea standardelor sau a specificațiilor tehnice care sunt relevante pentru sistem;

(c) interacțiunile și, după caz, stabilirea de legături cu părțile interesate relevante, inclusiv cu organizațiile de standardizare europene sau internaționale, inclusiv în scopul efectuării sau primirii de contribuții tehnice;

(d) emiterea de recomandări adresate Comisiei cu privire la îmbunătățirile și actualizările necesare ale sistemelor, inclusiv în vederea unei posibile revizuiri a sistemelor;

(e) schimbul de informații privind punerea în practică a sistemelor între statele membre;

(f) contribuții la mecanismele de revizuire *inter pares* și de evaluare *inter pares* și analize ale rezultatelor acestor evaluări pentru a îmbunătăți funcționarea sistemelor și pentru a sprijini posibila lor revizuire.

(5) ECCG poate emite un aviz cu privire la întreținerea sistemelor europene de certificare a securității cibernetice.

Articolul 76

Evaluarea, revizuirea și retragerea unui sistem european de certificare a securității cibernetice

(1) Cel puțin o dată la patru ani după intrarea în vigoare a unui sistem european de certificare a securității cibernetice, ENISA evaluează impactul și eficacitatea sistemului respectiv, în cooperare cu subgrupul de întreținere relevant al ECCG și ținând seama de feedbackul primit de la părțile interesate. ENISA efectuează evaluarea prin realizarea analizei de piață în conformitate cu articolul 8 alineatul (1).

(2) În urma evaluării menționate la alineatul (1), Comisia poate revizui sau retrage actele de punere în aplicare care prevăd un sistem european de certificare a securității cibernetice în temeiul articolului 74 alineatul (9).

(3) Atunci când revizuiește sau retrage sistemele europene de certificare a securității cibernetice, Comisia consultă ENISA, ECCG și subgrupul său de întreținere relevant și ține seama de opiniile părților interesate relevante și ale altor entități ale Uniunii.

(4) ECCG poate emite un aviz cu privire la revizuirea sau retragerea unui sistem european de certificare a securității cibernetice. Comisia ține seama în mod corespunzător de acesta atunci când revizuiește sau retrage sistemul european de certificare a securității cibernetice.

Articolul 77

Specificații tehnice în sistemele europene de certificare a securității cibernetice

(1) ENISA poate elabora specificații tehnice în vederea unui viitor sistem european de certificare a securității cibernetice sau pentru a sprijini menținerea unui sistem european de certificare a securității cibernetice.

(2) Specificațiile tehnice menționate la alineatul (1) de la prezentul articol se elaborează în timp util, cu sprijinul ECCG și al subgrupurilor sale de întreținere și, după caz, al grupului de lucru ad-hoc corespunzător, astfel cum se menționează la articolul 75 alineatul (3). În acest scop, ENISA solicită, de asemenea, contribuții din partea grupurilor relevante de părți interesate, ținând seama de strategia de întreținere menționată la articolul 75 alineatul (1).

(3) În cazul în care specificațiile tehnice sunt menționate într-un sistem european de certificare a securității cibernetice, astfel cum se menționează la articolul 74 alineatul (10), acestea sunt puse la dispoziție pe site-ul menționat la articolul 79.

(4) În cazuri justificate în mod corespunzător, în special în cazul în care specificațiile tehnice conțin informații care ar putea compromite securitatea produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate certificate sau a posturii certificate de securitate cibernetică a entităților, acestea sunt distribuite numai părților interesate vizate de cerințele sistemului. Aceste specificații tehnice nu trebuie să fie menționate într-un sistem european de certificare a securității cibernetice, astfel cum se menționează la articolul 74 alineatul (10).

Articolul 78

Facilitarea respectării legislației Uniunii

(1) În cazul în care un act juridic specific al Uniunii prevede acest lucru, un certificat eliberat în cadrul unui sistem european de certificare a securității cibernetice demonstrează conformitatea și conferă o prezumție de conformitate cu cerințele corespunzătoare prevăzute în actul juridic respectiv.

(2) Activitățile de evaluare din cadrul unui sistem european de certificare a securității cibernetice sunt în concordanță cu actul juridic corespunzător al Uniunii care stabilește demonstrarea conformității și prezumția de conformitate. În cazul în care astfel de activități de evaluare nu sunt specificate în actul juridic corespunzător al Uniunii, programul trebuie să le specifice. O evaluare a conformității pentru certificarea care conferă prezumția de conformitate cu cerințele prevăzute în legislația Uniunii trebuie să fie efectuată de un organism terț.

(3) În absența unei legislații armonizate la nivelul Uniunii, dreptul intern poate prevedea, de asemenea, că un sistem european de certificare a securității cibernetice poate fi utilizat pentru a demonstra conformitatea și pentru a stabili prezumția de conformitate cu cerințele legale specifice prevăzute în dreptul intern.

Articolul 79

Adoptarea sistemelor europene de certificare a securității cibernetice, site-ul ENISA și publicarea certificatelor

(1) ENISA organizează activități de promovare a adoptării sistemelor europene de certificare a securității cibernetice adoptate, inclusiv prin menținerea site-ului menționat la alineatul (2) de la prezentul articol.

(2) ENISA menține și actualizează periodic un site dedicat care oferă informații publice cu privire la următoarele:

(a) sistemele europene de certificare a securității cibernetice;

(b) taxele aferente întreținerii fiecărui sistem european de certificare a securității cibernetice;

(c) specificațiile tehnice relevante ale ENISA;

(d) certificatele europene de securitate cibernetică și declarațiile de conformitate UE, inclusiv informații cu privire la certificatele și declarațiile care nu mai sunt valabile sau care sunt suspendate, retrase sau expirate;

(e) informațiile suplimentare relevante în materie de securitate cibernetică furnizate în conformitate cu articolul 84;

(f) rezumatele evaluărilor *inter pares* în temeiul articolului 89 alineatul (7);

(g) specificațiile tehnice menționate într-un sistem european de certificare a securității cibernetice în temeiul articolului 74 alineatul (10).

(3) După caz, site-ul menționat la alineatul (2) indică și sistemele naționale de certificare a securității cibernetice care au fost înlocuite de un sistem european de certificare a securității cibernetice.

CAPITOLUL II
Conținutul sistemelor europene de certificare a securității cibernetice

Articolul 80
Obiectivele de securitate ale sistemelor europene de certificare a securității cibernetice

(1) Un sistem european de certificare a securității cibernetice urmărește, după caz, următoarele obiective de securitate:

(a) să asigure că produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate sunt securizate în mod implicit și începând cu momentul conceperii;

(b) să protejeze datele stocate, transmise sau prelucrate în alt mod împotriva stocării, prelucrării, accesării sau divulgării accidentale sau neautorizate prin mijloace tehnice adecvate, ținând seama de întregul ciclu de viață al produselor TIC, al serviciilor TIC sau al proceselor TIC;

(c) să protejeze integritatea datelor cu caracter personal sau a altor date, comenzi, programe și configurații stocate, transmise sau prelucrate în alt mod împotriva oricărei manipulări sau modificări neautorizate de utilizator și să raporteze cu privire la fișierele corupte, ținând seama de întregul ciclu de viață al produselor TIC, al serviciilor TIC sau al proceselor TIC;

(d) să asigure protecția împotriva accesului neautorizat prin mecanisme de control adecvate, inclusiv, dar fără a se limita la sistemele de autentificare, de gestionare a identității sau a accesului, și să raporteze privind posibilul acces neautorizat;

(e) să identifice și să documenteze componentele și vulnerabilitățile, inclusiv, după caz, prin întocmirea unei liste a materialelor software care să acopere cel puțin dependențele de nivel superior;

(f) să furnizeze informații legate de securitate prin înregistrarea și monitorizarea activității interne relevante, inclusiv accesul la date, servicii sau funcții sau modificarea acestora, după caz, cu un mecanism de neparticipare pentru utilizator;

(g) să verifice că produsele TIC, serviciile TIC și procesele TIC nu conțin vulnerabilități cunoscute care pot fi exploatate;

(h) să protejeze disponibilitatea funcțiilor esențiale și de bază, inclusiv după un incident, inclusiv prin reziliență și măsuri de atenuare împotriva atacurilor vizând blocarea accesului la servicii;

(i) să reducă la minimum a impactului negativ asupra disponibilității serviciilor furnizate de alte rețele și dispozitive în cazul unui incident fizic sau tehnic;

(j) să se asigure că produsele TIC, serviciile TIC și procesele TIC sunt testate periodic, iar securitatea lor este revizuită;

(k) să se asigure că vulnerabilitățile sunt abordate și remediate fără întârziere, inclusiv prin actualizări de securitate, și că informațiile privind vulnerabilitățile remediate sunt partajate și făcute publice, cu excepția cazului în care riscurile aferente publicării depășesc beneficiile în materie de securitate;

(l) să se asigure că există o politică privind divulgarea coordonată a vulnerabilităților;

(m) să faciliteze schimbul de informații cu privire la potențialele vulnerabilități ale produselor TIC, ale serviciilor TIC și ale proceselor TIC;

(n) să se asigure că, în cazul în care sunt disponibile actualizări de securitate pentru a aborda problemele de securitate identificate, respectivele actualizări de securitate sunt difuzate fără întârziere;

(o) să se asigure că serviciile de securitate gestionate sunt furnizate de personal care are competența, expertiza și experiența necesare, inclusiv un nivel suficient și adecvat de cunoștințe tehnice și competențe în domeniul specific, experiență suficientă și adecvată și cel mai înalt grad de integritate profesională;

(p) să se asigure că produsele TIC, serviciile TIC și procesele TIC utilizate pentru furnizarea serviciilor de securitate gestionate sunt securizate începând cu momentul conceperii și în mod implicit și, după caz, includ cele mai recente actualizări de securitate și nu conțin vulnerabilități cunoscute public;

(q) să se asigure că entitatea certificată dispune de proceduri interne adecvate pentru a se asigura că serviciile sunt furnizate la un nivel de calitate suficient și adecvat;

(r) să se asigure că entitatea certificată este în măsură să identifice incidentele, să se protejeze împotriva acestora, să le detecteze, să răspundă la acestea și să se redreseze în urma acestora;

(s) să se asigure că entitatea certificată este în măsură să gestioneze riscurile la adresa securității rețelelor și a sistemelor informatice utilizate de entitate pentru

operațiunile sale sau pentru furnizarea serviciilor sale și să prevină sau să reducă la minimum impactul incidentelor asupra destinatarilor serviciilor sale și asupra altor servicii;

(t) să se asigure că entitatea certificată este în măsură să își construiască, să își asigure și să își revizuiască integritatea operațională și fiabilitatea, asigurându-se, fie direct, fie indirect prin utilizarea serviciilor furnizate de furnizori terți de servicii TIC, că dispune de întreaga gamă de capacități legate de TIC necesare pentru a aborda securitatea rețelelor și a sistemelor informatice care sunt utilizate de entitate și care sprijină furnizarea continuă de servicii și calitatea acestora, inclusiv pe tot parcursul perturbărilor;

(u) să se asigure că entitatea certificată este în măsură să pună în aplicare și să mențină un sistem de management al securității informațiilor;

(v) să se opună oricărui eveniment care ar putea compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețeaua și sistemul informatic utilizate de entitate sau accesibile prin intermediul acestora și să asigure furnizarea continuă a serviciilor și calitatea acestora, inclusiv pe tot parcursul perturbărilor;

(w) să se asigure că entitatea este în măsură să asigure securitatea prelucrării datelor cu caracter personal.

(2) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 119 pentru a modifica alineatul (1) de la prezentul articol prin adăugarea sau modificarea obiectivelor de securitate, pentru a se asigura că acestea reflectă cele mai recente evoluții tehnologice și noile amenințări conexe, precum și prin adoptarea unei noi legislații a Uniunii care să stabilească demonstrarea conformității și prezumția de conformitate prin certificarea europeană de securitate cibernetică cu cerințele de securitate cibernetică relevante din legislația respectivă.

(3) Un sistem european de certificare a securității cibernetice care vizează produsele cu elemente digitale, astfel cum sunt definite la articolul 3 punctul 1 din Regulamentul (UE) 2024/2847, este conceput în conformitate cu cerințele esențiale de securitate cibernetică prevăzute în anexa I la regulamentul respectiv și ține seama de standardele armonizate disponibile.

Articolul 81

Elemente ale sistemelor europene de certificare a securității cibernetice

(1) Un sistem european de certificare a securității cibernetice include cel puțin următoarele:

(a) obiectul și domeniul de aplicare al sistemului de certificare, inclusiv tipul sau categoriile de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate sau activele, serviciile și funcțiile entității care intră în domeniul de aplicare al certificării;

(b) o descriere clară a scopului sistemului și, după caz, identificarea legislației Uniunii care stabilește cerințele pentru care certificatele europene de securitate cibernetică demonstrează conformitatea și conferă o prezumție de conformitate;

(c) strategia de întreținere care specifică abordarea activităților de întreținere prevăzute la articolul 75;

(d) cerințele specifice în materie de securitate cibernetică, criteriile și metodele de evaluare care trebuie utilizate pentru evaluarea produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate sau a posturii de securitate cibernetică a entităților, precum și trimiterile la standardele internaționale, europene sau naționale aplicate la evaluarea produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate sau a posturii cibernetice a entităților sau, în cazul în care astfel de standarde nu sunt disponibile sau adecvate, la specificațiile tehnice elaborate de ENISA în temeiul articolului 77 sau, în cazul în care astfel de specificații nu sunt disponibile, la alte specificații tehnice;

(e) perioada maximă de valabilitate a certificatelor europene de securitate cibernetică eliberate în temeiul sistemului;

(2) Un sistem european de certificare a securității cibernetice include cel puțin norme și condiții privind următoarele:

(a) monitorizarea conformității produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate sau a posturii de securitate cibernetică a entităților cu cerințele certificatelor europene de securitate cibernetică sau ale declarațiilor de conformitate UE, inclusiv mecanismele de demonstrare a conformității continue cu cerințele de securitate cibernetică specificate;

(b) eliberarea, confirmarea, retragerea și reînnoirea certificatelor europene de securitate cibernetică, extinderea sau reducerea domeniului de aplicare al certificării și recertificarea;

(c) consecințele neconformității produselor TIC, serviciilor TIC, proceselor TIC, serviciilor de securitate gestionate sau entităților care au fost certificate sau pentru care a fost eliberată o declarație de conformitate UE, dar care nu sunt conforme cu cerințele sistemului;

(d) modalitățile de raportare și soluționare a vulnerabilităților în materie de securitate cibernetică nedetectate anterior ale produselor TIC, serviciilor TIC și proceselor TIC;

(e) conținutul și formatul certificatelor europene de securitate cibernetică și ale declarațiilor de conformitate UE care urmează să fie eliberate;

(f) perioada de valabilitate a declarației de conformitate UE, documentația tehnică și toate celelalte informații relevante care trebuie să fie puse la dispoziție de producătorul sau de furnizorul de produse TIC, de servicii TIC, de procese TIC sau de servicii de securitate gestionate sau de entitatea a cărei postură de securitate cibernetică face obiectul certificării;

(g) orice mecanisme de evaluare *inter pares* instituite în cadrul sistemului pentru autoritățile sau organismele care eliberează certificate europene de securitate cibernetică în temeiul articolului 85 alineatul (4), care nu aduc atingere evaluării *inter pares* prevăzute la articolul 90;

(h) confidențialitatea informațiilor și a datelor obținute de toate părțile în îndeplinirea sarcinilor și a activităților legate de punerea în aplicare a dispozițiilor prevăzute în prezentul titlu;

(i) formatul și procedurile care trebuie urmate de producători sau de furnizori de produse TIC, de servicii TIC sau de procese TIC atunci când furnizează și actualizează informațiile suplimentare privind securitatea cibernetică în conformitate cu articolul 84 și

(j) continuitatea activităților de certificare în situații extraordinare de criză, care sunt inevitabile și împiedică posibilitatea de a aplica normele sistemului de certificare.

(3) Un sistem european de certificare a securității cibernetice include, după caz, și următoarele:

(a) unul sau mai multe niveluri de asigurare și nivelurile de evaluare corespunzătoare;

(b) profiluri de protecție pentru a specifica cerințele de securitate aplicabile unei anumite categorii de produse TIC, de servicii TIC, de procese TIC sau de servicii de securitate gestionate;

(c) extinderea profilurilor pentru a stabili cerințe de securitate suplimentare, inclusiv, după caz, cerințe de securitate prevăzute în dispozițiile naționale de transpunere a dreptului Uniunii;

(d) clarificarea activităților de evaluare a conformității, inclusiv calibrarea, testarea, certificarea și inspecția, pentru nivelul de asigurare „ridicat” sau în scopul demonstrării conformității și al acordării prezumției de conformitate, care sunt permise în afara Spațiului Economic European (SEE);

(e) identificarea sistemelor naționale sau internaționale de certificare a securității cibernetice care se referă la aceleași tipuri sau categorii de produse TIC, servicii TIC, procese TIC, servicii de securitate gestionate sau postură de securitate cibernetică a entităților;

(f) cerințe suplimentare sau specifice cărora se supun organismele de evaluare a conformității pentru a garanta competența tehnică a acestora de a evalua cerințele de securitate cibernetică;

(g) informațiile care sunt necesare pentru certificare și pe care un solicitant trebuie să le furnizeze sau să le pună în alt mod la dispoziția organismelor de evaluare a conformității;

(h) mărcile sau etichetele și condițiile în care pot fi utilizate aceste mărci sau etichete;

(i) condițiile pentru recunoașterea internațională a certificatelor europene de securitate cibernetică în conformitate cu articolul 87.

(4) Cerințele specificate ale sistemului european de certificare a securității cibernetice trebuie să fie conforme cu cerințele legislației Uniunii.

(5) Comisia este împuternicită să adopte acte de punere în aplicare de stabilire a unor principii comune și a unor modele de dispoziții pentru elementele prevăzute la alineatele (1), (2) și (3) în cadrul sistemelor europene de certificare a securității cibernetice. Dacă este cazul și dacă este disponibil, un sistem european de certificare a securității cibernetice poate include trimiteri la aceste principii și modele de dispoziții.

(6) Actele de punere în aplicare prevăzute la alineatul (5) se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2). Atunci când elaborează sau revizuiește principiile comune și modelele de dispoziții pentru elementele sistemelor europene de certificare a securității cibernetice, Comisia consultă ENISA și ia în considerare, după caz, opiniile exprimate de ECCG, de părțile interesate relevante și de alte organisme relevante.

Articolul 82
Nivelurile de asigurare și de evaluare ale sistemelor europene de certificare a securității cibernetice

(1) Un sistem european de certificare a securității cibernetice poate stabili unul sau mai multe dintre următoarele niveluri de asigurare pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura de securitate cibernetică a entităților: „de bază”, „substanțial” sau „ridicat”. Aceste niveluri de asigurare sunt proporționale cu nivelul de risc asociat cu utilizarea preconizată a produsului TIC, a serviciului TIC, a procesului TIC, a serviciului de securitate gestionat sau cu natura entităților a căror postură de securitate cibernetică face obiectul certificării și cu mediul lor operațional, în ceea ce privește probabilitatea și impactul unui incident.

(2) Certificatele europene de securitate cibernetică se referă la orice nivel de asigurare specificat în sistemul european de certificare a securității cibernetice în temeiul căruia sunt eliberate certificatele respective. Declarațiile de conformitate UE se referă la nivelul de asigurare „de bază”.

(3) Cerințele de securitate corespunzătoare fiecărui nivel de asigurare sunt prevăzute de sistemul european de certificare a securității cibernetice relevant, inclusiv controalele de securitate corespunzătoare și evaluarea corespunzătoare la care trebuie să fie supus produsul TIC, serviciul TIC, procesul TIC, serviciul de securitate gestionat sau postura de securitate cibernetică a entității.

(4) Certificatul european de securitate cibernetică sau declarația de conformitate UE face trimitere la specificații tehnice, standarde și proceduri conexe acestora, inclusiv controale tehnice, al căror scop este de a diminua riscul de incidente de securitate cibernetică sau de a le preîntâmpina.

(5) Un certificat european de securitate cibernetică sau o declarație de conformitate UE care face trimitere la nivelul de asigurare „de bază” oferă asigurare cu privire la faptul că produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura de securitate cibernetică a entităților pentru care se eliberează certificatul respectiv sau declarația de conformitate UE respectivă îndeplinesc cerințele de securitate corespunzătoare, inclusiv controalele de securitate, și că acestea au fost evaluate la un nivel care urmărește minimizarea riscurilor de bază cunoscute de incidente și de atacuri cibernetice. Activitățile de evaluare care trebuie să fie întreprinse includ cel puțin o examinare a documentației tehnice. În cazurile în care o astfel de examinare nu este adecvată, se desfășoară activități de evaluare înlocuitoare cu efect echivalent.

(6) Un certificat european de securitate cibernetică care face trimitere la nivelul de asigurare „substanțial” oferă asigurare cu privire la faptul că produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura de securitate cibernetică a entităților pentru care se eliberează certificatul respectiv îndeplinesc cerințele de securitate corespunzătoare, inclusiv controalele de securitate, și că acestea au fost evaluate la un nivel care urmărește minimizarea riscurilor

cunoscute de incidente și atacuri cibernetice și a riscului de atacuri cibernetice desfășurate de actori cu competențe și resurse limitate. Activitățile de evaluare care trebuie să fie întreprinse includ cel puțin o examinare pentru a demonstra absența vulnerabilităților cunoscute public și testarea pentru a demonstra că produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau entitățile implementează corect controalele de securitate necesare. În cazurile în care oricare dintre aceste activități de evaluare nu este adecvată, se desfășoară activități de evaluare înlocuitoare cu efect echivalent.

(7) Un certificat european de securitate cibernetică care face trimitere la nivelul de asigurare „ridicat” oferă asigurare cu privire la faptul că produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura de securitate cibernetică a entităților pentru care se eliberează certificatul respectiv îndeplinesc cerințele de securitate corespunzătoare, inclusiv controalele de securitate, și că acestea au fost evaluate la un nivel care urmărește minimizarea riscurilor de incidente și atacuri cibernetice de ultimă generație desfășurate de actori cu competențe și resurse semnificative. Activitățile de evaluare care trebuie întreprinse includ cel puțin următoarele:

(a) o examinare pentru a demonstra absența vulnerabilităților cunoscute public;

(b) testarea pentru a demonstra că produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau entitățile implementează corect controalele de securitate necesare, la nivel de ultimă generație;

(c) o evaluare a rezistenței produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate sau a entităților la atacatori calificați, utilizând, după caz, teste de penetrare.

În cazurile în care oricare dintre aceste activități de evaluare nu este adecvată, se desfășoară activități înlocuitoare cu efect echivalent. Orice activități de evaluare a conformității, inclusiv calibrarea, testarea, certificarea și inspecția, pentru nivelul de asigurare „ridicat” se desfășoară în Spațiul Economic European, cu excepția cazului în care se prevede altfel într-un sistem european de certificare a securității cibernetice.

(8) În cazul în care un sistem european de certificare a securității cibernetice este conceput pentru a demonstra conformitatea și a acorda prezumția de conformitate cu un act juridic specific al Uniunii, un certificat european de securitate cibernetică oferă asigurarea că produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate certificate sau postura de securitate cibernetică certificată a entităților îndeplinesc cerințele de securitate cibernetică corespunzătoare din actul juridic respectiv. Orice activități de evaluare a conformității, inclusiv calibrarea, testarea, certificarea și inspecția, în scopul prezumției de conformitate se desfășoară în Spațiul Economic European, cu excepția cazului în care se prevede altfel într-un sistem european de certificare a securității cibernetice.

(9) Un sistem european de certificare a securității cibernetice poate specifica mai multe niveluri de evaluare pentru un anumit nivel de asigurare. Fiecare dintre nivelurile de evaluare corespunde unuia dintre nivelurile de asigurare.

Articolul 83
Autoevaluarea conformității

(1) Un sistem european de certificare a securității cibernetice poate permite autoevaluarea conformității pe răspunderea exclusivă a producătorului sau a furnizorului de produse TIC, servicii TIC, procese TIC, servicii de securitate gestionate sau a entității a cărei postură de securitate cibernetică face obiectul certificării. Autoevaluarea conformității este permisă numai în cazul produselor TIC, serviciilor TIC, proceselor TIC, serviciilor de securitate gestionate sau al posturii de securitate cibernetică a entităților care prezintă un risc redus corespunzând nivelului de asigurare „de bază”.

(2) Producătorul sau furnizorul de produse TIC, servicii TIC, procese TIC, servicii de securitate gestionate sau entitatea a cărei postură de securitate cibernetică face obiectul certificării poate emite o declarație de conformitate UE care să ateste că a fost demonstrată îndeplinirea cerințelor prevăzute în sistemul european de certificare a securității cibernetice. Prin eliberarea unei astfel de declarații, producătorul, furnizorul sau entitatea respectivă își asumă responsabilitatea pentru conformitatea produsului TIC, a serviciului TIC, a procesului TIC, a serviciului de securitate gestionat sau a posturii de securitate cibernetică cu cerințele prevăzute în sistemul respectiv.

(3) Producătorul sau furnizorul de produse TIC, servicii TIC, procese TIC, servicii de securitate gestionate sau entitatea a cărei postură de securitate cibernetică face obiectul certificării pune declarația de conformitate UE, documentația tehnică și toate celelalte informații relevante referitoare la conformitatea produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate sau a posturii de securitate cibernetică cu sistemul european de certificare a securității cibernetice la dispoziția autorității naționale de certificare a securității cibernetice desemnate în temeiul articolului 89 pentru perioada prevăzută în sistemul respectiv. O copie a declarației de conformitate UE se transmite fără întârzieri nejustificate către autoritatea națională de certificare a securității cibernetice și către ENISA.

Articolul 84
Informații suplimentare privind securitatea cibernetică pentru produsele TIC, serviciile TIC și procesele TIC certificate

(1) Producătorul sau furnizorul de produse TIC, servicii TIC sau procese TIC pentru care a fost eliberată o declarație de conformitate UE sau un certificat european de securitate cibernetică trebuie să pună la dispoziția utilizatorului următoarele informații suplimentare în materie de securitate cibernetică:

(a) scopul preconizat al produsului TIC, al serviciului TIC sau al procesului TIC relevant, inclusiv mediul de securitate furnizat de producător sau de furnizor;

(b) orientări și recomandări care să le servească utilizatorilor la configurarea, instalarea, derularea, funcționarea și întreținerea securizate ale produselor TIC sau serviciilor TIC;

(c) tipul de asistență tehnică de securitate oferită de producător sau de furnizor și data de încheiere a perioadei de asistență în care utilizatorii se pot aștepta să fie gestionate vulnerabilitățile și să primească actualizări de securitate;

(d) în cazul în care producătorul sau furnizorul decide să pună la dispoziția utilizatorului o listă a materialelor software, informații cu privire la locul în care aceasta poate fi accesată.

(2) Producătorul sau furnizorul de produse TIC, servicii TIC sau procese TIC pentru care a fost eliberată o declarație de conformitate UE sau un certificat european de securitate cibernetică trebuie să pună la dispoziția publicului următoarele informații suplimentare în materie de securitate cibernetică:

(a) ghișeul unic unde pot fi raportate și primite informații cu privire la vulnerabilități, precum și locul în care poate fi găsită politica producătorului privind divulgarea coordonată a vulnerabilităților;

(b) informații cu privire la vulnerabilitățile remediate, inclusiv o descriere a vulnerabilităților, incluzând informații care să permită utilizatorilor să identifice produsul cu elemente digitale afectat, impactul vulnerabilităților, gravitatea acestora și informații clare și accesibile care să ajute utilizatorii să remedieze vulnerabilitățile; în cazuri justificate în mod corespunzător, atunci când producătorii consideră că riscurile de securitate ale publicării depășesc beneficiile în materie de securitate, aceștia pot amâna publicarea informațiilor cu privire la o vulnerabilitate fixă până după ce utilizatorilor li s-a oferit posibilitatea de a aplica corecția relevantă;

(3) Informațiile menționate la alineatele (1) și (2) se pun la dispoziție în format electronic și rămân disponibile și sunt actualizate, după caz, pe durata valabilității și cel puțin pentru o perioadă de cinci ani de la expirarea sau retragerea certificatului european de securitate cibernetică sau a declarației de conformitate UE relevante.

(4) Obligațiile prevăzute la alineatele (1) și (2) nu se aplică în cazul în care securitatea produsului TIC, a serviciului TIC sau a procesului TIC relevant ar putea fi compromisă dacă informațiile sunt puse la dispoziția publicului.

CAPITOLUL III
Guvernanța cadrului european de certificare a securității cibernetice

Secțiunea 1
Normele generale și gestionarea sistemelor europene de certificare a securității cibernetice

Articolul 85
Eliberarea certificatelor europene de securitate cibernetică

(1) Se consideră că produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura de securitate cibernetică a entităților care au fost certificate în cadrul unui sistem european de certificare a securității cibernetice sunt conforme cu cerințele unui astfel de sistem.

(2) Organismele de evaluare a conformității menționate la articolul 91 eliberează certificate europene de securitate cibernetică pe baza criteriilor incluse în sistemul european de certificare a securității cibernetice adoptat în temeiul articolului 74.

(3) Prin derogare de la alineatul (2), un sistem european de certificare a securității cibernetice poate prevedea ca certificatele europene de securitate cibernetică ce

rezultă din sistemul respectiv să fie eliberate numai de unul dintre următoarele organisme publice:

(a) o autoritate națională de certificare a securității cibernetice menționată la articolul 88 care este acreditată ca organism de evaluare a conformității în temeiul articolului 91 alineatul (1);

(b) un organism public care este acreditat ca organism de evaluare a conformității în temeiul articolului 91 alineatul (1).

(4) În cazul în care un sistem european de certificare a securității cibernetice adoptat în temeiul articolului 74 stabilește un nivel de asigurare „ridicat” sau în cazul în care un astfel de sistem prevede în mod specific altfel, certificatul european de securitate cibernetică din cadrul sistemului respectiv se eliberează numai de către o autoritate națională de certificare a securității cibernetice menționată la articolul 88 care este acreditată ca organism de evaluare a conformității în temeiul articolului 91 alineatul (1) sau în următoarele cazuri:

(a) de către un organism de evaluare a conformității pe baza unui model de aprobare prealabilă sau

(b) de către un organism de evaluare a conformității pe baza unui model general de delegare.

(5) Comisia este împuternicită să adopte acte de punere în aplicare care să precizeze procedurile de aprobare prealabilă sau modelele generale de delegare menționate la alineatul (4) de la prezentul articol. În procesul de elaborare a respectivelor acte de punere în aplicare, Comisia consultă ECCG. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2).

(6) Persoana fizică sau juridică care supune certificării produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate sau entitatea care solicită certificarea posturii sale de securitate cibernetică trebuie să pună la dispoziția autorității naționale de certificare a securității cibernetice desemnate în temeiul articolului 89, în cazul în care autoritatea respectivă este organismul care eliberează certificatul european de securitate cibernetică, sau a organismului de evaluare a conformității menționat la articolul 91, toate informațiile necesare pentru efectuarea certificării.

(7) Organismele de evaluare a conformității și, după caz, autoritățile naționale de certificare a securității cibernetice informează ENISA fără întârzieri nejustificate cu privire la deciziile lor care afectează statutul certificatelor europene de securitate cibernetică și al declarațiilor de conformitate UE în conformitate cu articolul 94.

(8) Deținătorul unui certificat european de securitate cibernetică informează organismul de evaluare a conformității și, după caz, autoritatea națională de certificare a securității cibernetice, menționate la alineatul (7), cu privire la orice vulnerabilități sau neconformități detectate ulterior în ceea ce privește produsul TIC, serviciul TIC, procesul TIC, serviciul de securitate gestionat sau postura de securitate cibernetică certificată a entității care au un impact probabil asupra conformității sale cu certificatul. Organismul respectiv transmite informațiile respective fără întârzieri nejustificate autorității naționale de certificare a securității cibernetice în cauză și evaluează impactul asupra certificatului în conformitate cu condițiile sistemului menționate la articolul 81 alineatul (2) litera (d).

(9) Pentru produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate certificate ale acestora, identificate, în totalitate sau parțial, ca active esențiale în temeiul articolului 102, deținătorii unui certificat european de securitate cibernetică nu utilizează, nu instalează și nu integrează în alt mod componente TIC sau componente TIC care includ componente TIC de la furnizori cu grad ridicat de risc în produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate certificate.

(10) Certificatele europene de securitate cibernetică se eliberează pentru durata prevăzută de sistemul european de certificare a securității cibernetice și pot fi reînnoite numai dacă sunt îndeplinite în continuare cerințele relevante.

(11) Comisia cooperează cu statele membre pentru a asigura aplicarea dispozițiilor referitoare la eliberarea certificatelor europene de securitate cibernetică și în vederea aplicării articolului 100 alineatul (4) litera (b). Organismul de evaluare a conformității și, după caz, autoritatea națională de certificare a securității cibernetice furnizează Comisiei, la cerere și fără întârzieri nejustificate, toate informațiile referitoare la eliberarea certificatelor europene de securitate cibernetică sau a declarațiilor de conformitate UE relevante.

Articolul 86

Sistemele și certificatele naționale de certificare a securității cibernetice

(1) Sistemele naționale de certificare a securității cibernetice și procedurile aferente pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate și postura de securitate cibernetică a entităților care fac obiectul unui sistem european de certificare a securității cibernetice și sunt vizate de domeniul de aplicare al acestuia încetează să mai producă efecte de la data stabilită în actul de punere în aplicare adoptat în temeiul articolului 74 alineatul (9). Sistemele naționale de certificare a securității cibernetice și procedurile aferente pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate și postura de securitate cibernetică a entităților care fac obiectul unui sistem european de certificare a securității cibernetice și sunt vizate de domeniul de aplicare al acestuia își pot continua existența.

(2) Statele membre nu introduc noi sisteme naționale de certificare a securității cibernetice sau proceduri conexe pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate și postura de securitate cibernetică a entităților care fac deja obiectul unui sistem european de certificare a securității cibernetice și sunt vizate de domeniul de aplicare al acestuia.

(3) Certificatele existente care au fost eliberate în temeiul sistemelor naționale de certificare a securității cibernetice și care fac obiectul unui sistem european de certificare a securității cibernetice și sunt vizate de domeniul de aplicare al acestuia rămân valabile până la data expirării lor.

(4) Statele membre notifică Comisia și ECCG înainte de a adopta noi sisteme naționale de certificare a securității cibernetice pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate și postura de securitate cibernetică a entităților.

(5) Comisia poate sugera unui stat membru să retragă un sistem național de certificare a securității cibernetice pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura de securitate cibernetică a entităților, în cazul în

care dezvoltarea unui sistem european de certificare a securității cibernetice care să acopere aceste produse, servicii, procese sau postură de securitate cibernetică a fost deja solicitată în conformitate cu articolul 73, ținând seama de planul de dezvoltare a unui astfel de sistem.

Articolul 87

Recunoașterea internațională a certificatelor europene de securitate cibernetică

(1) Certificatele țărilor terțe pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate și postura de securitate cibernetică a entităților pot fi recunoscute, prin intermediul unui act de punere în aplicare sau prin încheierea unui acord între Uniune și țara terță în cauză sau o organizație internațională, ca fiind echivalente cu certificatele europene de securitate cibernetică în cazul în care cerințele sistemului relevant al țării terțe sau ale sistemului relevant al organizației internaționale sunt considerate echivalente cu cele ale sistemelor europene de certificare a securității cibernetice. Comisia este împuternicită să adopte astfel de acte de punere în aplicare. Actele de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2).

(2) Actele de punere în aplicare și acordurile menționate la alineatul (1) se bazează pe condițiile de recunoaștere internațională a certificatelor europene de securitate cibernetică stabilite în conformitate cu articolul 74 alineatul (11).

(3) Acordurile privind recunoașterea certificatelor țărilor terțe sau a certificatelor organizațiilor internaționale menționate la alineatul (1) se încheie numai dacă acestea recunosc, de asemenea, certificatele europene de securitate cibernetică ca fiind echivalente cu certificatele țărilor terțe.

Articolul 88

Autoritățile naționale de certificare a securității cibernetice

(1) Fiecare stat membru desemnează pe teritoriul său una sau mai multe autorități naționale de certificare a securității cibernetice sau, cu acordul unui alt stat membru, una sau mai multe autorități naționale de certificare a securității cibernetice din celălalt stat membru pentru a fi responsabile de atribuțiile de supraveghere în statul membru care face desemnarea.

(2) Fiecare stat membru informează Comisia cu privire la identitatea autorităților naționale de certificare a securității cibernetice desemnate. În cazul în care un stat membru desemnează mai multe autorități, acesta informează Comisia și cu privire la sarcinile atribuite fiecăreia dintre respectivele autorități.

(3) Fiecare autoritate națională de certificare a securității cibernetice este independentă de entitățile pe care le supraveghează în ceea ce privește organizarea, deciziile de finanțare, structura juridică și procesul decizional.

(4) Activitățile autorităților naționale de certificare a securității cibernetice care se referă la eliberarea de certificate europene de securitate cibernetică în temeiul prezentului regulament trebuie să fie strict separate de activitățile lor de supraveghere prevăzute la prezentul articol și la articolul 85 alineatul (4) literele (a) și (b) și să se desfășoare independent unele de altele.

(5) Statele membre se asigură că autoritățile naționale de certificare a securității cibernetice dispun de resursele adecvate pentru a-și exercita competențele și pentru a-și îndeplini cu eficacitate și în mod eficient sarcinile.

(6) Autoritățile naționale de certificare a securității cibernetice au următoarele sarcini:

(a) participă la ECCG în temeiul articolului 90 alineatul (2);

(b) supraveghează și asigură respectarea normelor incluse în sistemele europene de certificare a securității cibernetice în temeiul articolului 81 alineatul (2) litera (a), pentru a asigura conformitatea produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate și a posturii de securitate cibernetică a entităților cu cerințele certificatelor europene de securitate cibernetică care au fost emise pe teritoriile lor respective, în cooperare cu autoritățile relevante de supraveghere a pieței sau cu autoritățile de supraveghere, inclusiv cu autoritățile competente în temeiul Directivei (UE) 2022/2555 a Parlamentului European și a Consiliului[82] sau al Regulamentului (UE) 2024/2847;

(c) monitorizează, în cooperare cu autoritățile relevante de supraveghere a pieței, respectarea și asigurarea respectării obligațiilor producătorilor sau furnizorilor de produse TIC, servicii TIC, procese TIC, servicii de securitate gestionate sau ale entităților a căror postură de securitate cibernetică este certificată, prevăzute în prezentul regulament, care sunt stabiliți pe teritoriile lor respective și care efectuează autoevaluarea conformității în sistemul european de certificare a securității cibernetice corespunzător;

(d) fără a aduce atingere articolului 91 alineatul (3), asistă și sprijină activ organismele naționale de acreditare sau alte autorități relevante la monitorizarea și supravegherea activităților organismelor de evaluare a conformității în sensul prezentului regulament;

(e) cooperează cu Comisia în cazul în care competența unui organism de evaluare a conformității este contestată în temeiul articolului 94;

(f) monitorizează și supraveghează activitățile organismelor publice menționate la articolul 85 alineatul (3);

(g) după caz, autorizează organismele de evaluare a conformității în conformitate cu articolul 93, monitorizează respectarea obligațiilor organismelor de evaluare a conformității și asigură respectarea de către acestea a cerințelor suplimentare sau specifice prevăzute în sistemele europene de certificare a securității cibernetice în temeiul articolului 81 alineatul (3) litera (f) și restricționează, suspendă sau retrage autorizația existentă în cazul în care organismele de evaluare a conformității nu îndeplinesc cerințele prezentului regulament;

(h) gestionează plângerile persoanelor fizice sau juridice în legătură cu certificatele europene de securitate cibernetică eliberate de autoritățile naționale de certificare a securității cibernetice sau cu cele eliberate de organismele de

[82] Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (JO L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

evaluare a conformității în conformitate cu articolul 85 alineatul (4), sau în legătură cu declarațiile de conformitate UE eliberate în temeiul articolului 83, investighează, în măsura în care este oportun, subiectul plângerii și informează reclamantul despre stadiul și rezultatul investigației, într-un termen rezonabil;

(i) prezintă Comisiei, ENISA și ECCG un raport anual cu privire la principalele sale activități până la data de 31 martie [anul intrării în vigoare + 12 luni] a fiecărui an și pune aceste rapoarte la dispoziția echipei de evaluare *inter pares* în cazul în care autoritatea națională de certificare a securității cibernetice face obiectul unei evaluări *inter pares* în conformitate cu articolul 89;

(j) cooperează cu alte autorități naționale de certificare a securității cibernetice, autorități de supraveghere a pieței sau cu alte autorități publice, inclusiv prin schimbul de informații cu privire la o posibilă neconformitate a produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate și a posturii de securitate cibernetică a entităților cu cerințele prezentului regulament sau cu cerințele sistemului european de certificare a securității cibernetice specific;

(k) monitorizează evoluțiile relevante din domeniul certificării securității cibernetice.

(7) Fiecare autoritate națională de certificare a securității cibernetice dispune cel puțin de următoarele competențe:

(a) competența de a cere organismelor de evaluare a conformității, deținătorilor de certificate europene de securitate cibernetică și entităților care eliberează declarații de conformitate UE să furnizeze toate informațiile care îi sunt necesare pentru îndeplinirea atribuțiilor sale;

(b) competența de a efectua investigații, sub formă de audituri, asupra organismelor de evaluare a conformității, a deținătorilor de certificate europene de securitate cibernetică și a entităților care eliberează declarații de conformitate UE pentru a verifica conformitatea acestora cu cerințele prevăzute în prezentul titlu;

(c) competența de a lua măsuri adecvate, în conformitate cu dreptul intern, pentru a se asigura că organismele de evaluare a conformității, deținătorii de certificate europene de securitate cibernetică și entitățile care eliberează declarații de conformitate UE respectă prezentul regulament sau un sistem european de certificare a securității cibernetice;

(d) competența de a obține acces la sediile oricărui organism de evaluare a conformității sau al deținătorilor de certificate europene de securitate cibernetică cu scopul de a desfășura investigații în conformitate cu legislația Uniunii sau cu dreptul procedural național;

(e) competența de a retrage, în conformitate cu dreptul intern, certificatele europene de securitate cibernetică eliberate de autoritățile naționale de certificare a securității cibernetice sau de organismele de evaluare a conformității în conformitate cu articolul 85 alineatul (4), atunci când astfel de certificate nu sunt conforme cu prezentul regulament sau cu un sistem european de certificare a securității cibernetice;

(f) competența de a impune sancțiuni, în conformitate cu dreptul intern, astfel cum se prevede la articolul 97, și de a cere încetarea imediată a încălcărilor obligațiilor prevăzute de prezentul regulament.

(8) Autoritățile naționale de certificare a securității cibernetice cooperează între ele și cu Comisia, în special prin schimb de informații, de experiență și de bune practici în ceea ce privește certificarea securității cibernetice și aspectele tehnice privind securitatea cibernetică a produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate și a posturii cibernetice a entităților.

(9) Până la [data intrării în vigoare + 6 luni], ENISA elaborează un model pentru raportul menționat la alineatul (6) litera (i) de la prezentul articol, în cooperare cu Comisia și cu ECCG.

Articolul 89
Evaluarea inter pares

(1) Autoritățile naționale de certificare a securității cibernetice fac obiectul unei evaluări *inter pares*.

(2) Evaluarea *inter pares* se efectuează pe baza unor criterii și proceduri de evaluare clare și transparente, în special în privința cerințelor structurale, de resurse umane și de proces, a confidențialității și a plângerilor.

(3) Evaluarea *inter pares* examinează următoarele aspecte:

(a) după caz, dacă activitățile autorităților naționale de certificare a securității cibernetice legate de eliberarea certificatelor europene de securitate cibernetică menționate în prezentul regulament sunt strict separate de activitățile de supraveghere prevăzute la articolul 88 și dacă activitățile respective sunt desfășurate independent una de cealaltă;

(b) procedurile de supraveghere și de asigurare a respectării normelor de monitorizare a conformității produselor TIC, serviciilor TIC, proceselor TIC, serviciilor de securitate gestionate și a posturii de securitate cibernetică a entităților cu certificatele europene de securitate cibernetică în temeiul articolului 88 alineatul (7) litera (a);

(c) procedurile de monitorizare și de asigurare a respectării obligațiilor producătorilor și ale furnizorilor de produse TIC, de servicii TIC, de procese TIC sau de servicii de securitate gestionate sau alte entităților a căror postură de securitate cibernetică este certificată, în conformitate cu articolul 88 alineatul (7) litera (b);

(d) procedurile de monitorizare, de autorizare și de supraveghere a activităților desfășurate de organismele de evaluare a conformității.

(4) Evaluarea *inter pares* se efectuează cel puțin o dată la cinci ani de către cel puțin două autorități naționale de certificare a securității cibernetice din alte state membre și de către Comisie. ENISA participă, de asemenea, la evaluarea *inter pares* în calitate de observator. Echipa de evaluare *inter pares* întocmește raportul final și rezumatul evaluării *inter pares*.

(5) ENISA sprijină organizarea mecanismului de evaluare *inter pares* și a evaluărilor *inter pares*, inclusiv prin elaborarea de documente de orientare și modele relevante, în cooperare cu Comisia și cu ECCG.

(6) Comisia este împuternicită să adopte acte de punere în aplicare prin care să stabilească un plan pentru evaluarea *inter pares*, care acoperă o perioadă de cel puțin cinci ani, și să definească criterii privind componența echipei de evaluare *inter pares*, metodologia utilizată pentru evaluarea *inter pares*, calendarul, frecvența și alte atribuții legate de evaluarea *inter pares*. La elaborarea respectivelor acte de punere în aplicare, Comisia consultă ECCG și ENISA. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2).

(7) Raportul final, inclusiv posibilele orientări sau recomandări, și rezumatul evaluării *inter pares* sunt examinate de ECCG, care aprobă rezumatul în vederea publicării pe site-ul menționat la articolul 79 alineatul (2).

Articolul 90
Grupul european pentru certificarea securității cibernetice

(1) Se instituie Grupul european pentru certificarea securității cibernetice (ECCG).

(2) ECCG este compus din reprezentanți ai autorităților naționale de certificare a securității cibernetice sau din reprezentanți ai altor autorități naționale relevante. Niciun membru ECCG nu poate reprezenta mai mult de două state membre.

(3) ECCG are următoarele atribuții:

(a) să acorde consiliere și asistență Comisiei în activitatea sa de asigurare a punerii în aplicare și a aplicării coerente a normelor prevăzute în prezentul titlu, a aspectelor legate de politica de certificare a securității cibernetice și a coordonării abordărilor de politică;

(b) să acorde consiliere și asistență Comisiei la pregătirea cererilor de sisteme europene de certificare a securității cibernetice în temeiul articolului 73;

(c) să acorde asistență și consiliere ENISA și să coopereze cu aceasta în ceea ce privește pregătirea unei propuneri de sistem în temeiul articolului 74 și a specificațiilor tehnice în temeiul articolului 77;

(d) să acorde asistență și consiliere ENISA și să coopereze cu aceasta și cu Comisia în ceea ce privește activitățile de întreținere în temeiul articolului 75;

(e) să acorde asistență și consiliere Comisiei și să coopereze cu aceasta în ceea ce privește revizuirea sau retragerea sistemelor europene de certificare a securității cibernetice existente în temeiul articolului 76;

(f) să sugereze transmiterea către Comisie a unei cereri cu privire la pregătirea unei propuneri de sistem european de certificare a securității cibernetice în temeiul articolului 73 alineatul (2);

(g) să adopte avize adresate Comisiei cu privire la întreținerea, revizuirea și retragerea sistemelor europene de certificare a securității cibernetice existente;

(h) să examineze evoluțiile relevante în domeniul certificării de securitate cibernetică, inclusiv la nivel național în temeiul articolului 86, și să facă schimb de informații și de bune practici cu privire la sistemele de certificare a securității cibernetice;

(i) să faciliteze cooperarea dintre autoritățile naționale de certificare a securității cibernetice în temeiul normelor prevăzute în prezentul titlu prin consolidarea

capacităților și schimbul de informații, în special în ceea ce privește aspectele legate de certificarea securității cibernetice;

(j) să sprijine punerea în aplicare a mecanismului de evaluare *inter pares* în temeiul articolului 89 și a mecanismelor de evaluare *inter pares* în conformitate cu normele stabilite în cadrul unui sistem european de certificare a securității cibernetice în temeiul articolului 81 alineatul (2) litera (g);

(k) să faciliteze alinierea sistemelor europene de certificare a securității cibernetice la standardele recunoscute la nivel internațional, inclusiv ca parte a întreținerii sistemelor europene de certificare a securității cibernetice existente și, după caz, să facă recomandări ENISA pentru a colabora cu organizațiile de standardizare europene sau internaționale relevante pentru a remedia insuficiențele sau lacunele standardelor europene sau recunoscute la nivel internațional disponibile.

(4) Cu sprijinul ENISA, Comisia prezidează ECCG și asigură secretariatul ECCG.

(5) Comisia poate înființa subgrupuri ECCG pentru oricare dintre următoarele scopuri:

(a) să examineze chestiuni specifice pe baza termenilor de referință stabiliți de Comisie;

(b) să întrețină și să revizuiască sistemele europene de certificare în conformitate cu prezentul regulament și pe baza termenilor de referință stabiliți de Comisie.

(6) Subgrupurile raportează ECCG.

(7) Subgrupurile sunt coprezidate de Comisie și ENISA, iar secretariatul subgrupurilor este asigurat de ENISA.

(8) ECCG și subgrupurile sale adoptă regulamentul de procedură cu majoritatea simplă a membrilor lor, pe baza unei propuneri din partea Comisiei și cu acordul acesteia.

Secțiunea 2
Organisme de evaluare a conformității

Articolul 91
Competența organismelor de evaluare a conformității

(1) Organismele de evaluare a conformității sunt acreditate de organismele naționale de acreditare desemnate în temeiul Regulamentului (CE) nr. 765/2008. Acreditarea respectivă se eliberează numai dacă organismul național de acreditare îndeplinește cerințele stabilite în anexa I la prezentul regulament.

(2) În cazurile în care un certificat european de securitate cibernetică este eliberat de o autoritate națională de certificare a securității cibernetice în temeiul prezentului regulament, organismul de certificare al autorității naționale de certificare a securității cibernetice este acreditat ca organism de evaluare a conformității în temeiul alineatului (1).

(3) Acreditarea menționată la alineatul (1) se eliberează organismelor de evaluare a conformității pentru o perioadă de maximum cinci ani și poate fi reînnoită numai dacă organismul de evaluare a conformității îndeplinește cerințele prevăzute la prezentul articol. Organismele naționale de acreditare iau toate măsurile corespunzătoare într-un termen rezonabil pentru a restricționa, a suspenda sau a

revoca acreditarea unui organism de evaluare a conformității eliberată în temeiul alineatului (1) în cazul în care condițiile de acreditare nu sunt sau nu mai sunt îndeplinite sau în cazul în care organismul de evaluare a conformității nu respectă prezentul regulament.

(4) Atunci când se stabilesc cerințe de acreditare suplimentare sau specifice pentru un sistem european de certificare a securității cibernetice care acoperă produse TIC, în temeiul articolului 92, se urmăresc sinergii, după caz, cu cerințele referitoare la organismele notificate în temeiul Regulamentului (UE) 2024/2847 și cu cerințele de acreditare din cadrul sistemelor de certificare a securității cibernetice care au fost deja adoptate.

(5) În cazul în care un organism de evaluare a conformității este acreditat în conformitate cu Regulamentul (UE) 2024/2847, autoritățile relevante pot reutiliza rezultatele procesului de acreditare anterior în ceea ce privește orice suprapunere a cerințelor ca dovadă în cursul procesului de acreditare în temeiul prezentului regulament.

Articolul 92

Armonizarea suplimentară a competenței organismelor de evaluare a conformității

(1) În cazul în care un sistem european de certificare a securității cibernetice stabilește cerințe suplimentare sau specifice în temeiul articolului 81 alineatul (3) litera (f), organismele de evaluare a conformității sunt autorizate de o autoritate națională de certificare a securității cibernetice desemnată în temeiul articolului 88 alineatul (1) să îndeplinească sarcini în cadrul unui astfel de sistem. O astfel de autorizație se eliberează numai în cazul în care organismul de evaluare a conformității a fost acreditat și îndeplinește cerințele suplimentare sau specifice prevăzute în cadrul sistemului european de certificare a securității cibernetice.

(2) În cazul în care un organism de evaluare a conformității solicită o autorizație în temeiul prezentului articol, acesta transmite cererea autorității naționale de certificare a securității cibernetice din statul membru în care este stabilit sau autorității naționale de certificare a securității cibernetice la care a recurs statul membru respectiv în conformitate cu articolul 88 alineatul (1).

(3) Un organism de evaluare a conformității poate solicita o autorizație din partea unei autorități naționale de certificare a securității cibernetice, alta decât cea menționată la alineatul (2), în oricare dintre următoarele situații:

(a) în cazul în care autoritatea națională de certificare a securității cibernetice menționată la alineatul (1) nu efectuează autorizarea în ceea ce privește activitățile de evaluare a conformității pentru care se solicită autorizarea;

(b) în cazul în care autoritatea națională de certificare a securității cibernetice menționată la alineatul (1) nu a făcut obiectul unei evaluări *inter pares* în conformitate cu articolul 89 în ceea ce privește activitățile de evaluare a conformității pentru care se solicită autorizarea.

(4) În cazul în care o autoritate națională de certificare a securității cibernetice primește o cerere în temeiul alineatului (3), aceasta informează autoritatea națională de certificare a securității cibernetice a statului membru în care este stabilit organismul de evaluare a conformității solicitant. În aceste cazuri, autoritatea națională de certificare a securității cibernetice din statul membru respectiv poate participa la autorizare în calitate de observator.

(5) O autoritate națională de certificare a securității cibernetice poate solicita unei alte autorități naționale de certificare a securității cibernetice să efectueze părți ale activității de evaluare. În acest caz, certificatul de autorizare este eliberat de autoritatea solicitantă.

(6) Autorizația menționată la alineatul (1) este valabilă pentru o perioadă care nu depășește perioada de valabilitate a acreditării și poate fi reînnoită cu condiția ca organismul de evaluare a conformității să îndeplinească cerințele prevăzute la alineatul (1) și ca acreditarea sa să fi fost, de asemenea, reînnoită.

(7) Autoritățile naționale de certificare a securității cibernetice iau, într-un interval de timp rezonabil, toate măsurile corespunzătoare pentru a restricționa, a suspenda sau a revoca autorizația unui organism de evaluare a conformității eliberată în temeiul alineatului (1) în cazul în care condițiile de autorizare nu au fost îndeplinite sau nu mai sunt îndeplinite sau în cazul în care organismul de evaluare a conformității nu respectă prezentul regulament.

(8) Comisia este împuternicită să adopte acte de punere în aplicare pentru a stabili procedurile, inclusiv în ceea ce privește cooperarea transfrontalieră, de autorizare a organismelor de evaluare a conformității. În procesul de elaborare a actelor de punere în aplicare, Comisia consultă ENISA și ECCG. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2).

Articolul 93
Notificarea organismelor de evaluare a conformității

(1) Pentru fiecare sistem european de certificare a securității cibernetice, autoritățile naționale de certificare a securității cibernetice ale unui stat membru notifică Comisiei și celorlalte state membre organismele de evaluare a conformității care au fost acreditate și, după caz, autorizate în temeiul articolului 92.

(2) Autoritățile naționale de certificare a securității cibernetice efectuează notificarea menționată la alineatul (1) utilizând instrumentul de notificare electronică dezvoltat și gestionat de Comisie.

(3) Comisia este împuternicită să adopte acte de punere în aplicare pentru a stabili circumstanțele, formatele și procedurile pentru notificările menționate la alineatul (1) de la prezentul articol, inclusiv procedura de opoziție a altor state membre în cursul procesului de notificare, identificarea unică a organismelor de evaluare a conformității, precum și circumstanțele pentru restricționarea, suspendarea sau retragerea notificării. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2).

Articolul 94
Provocări în ceea ce privește competența organismelor de evaluare a conformității

(1) Comisia investighează toate cazurile în care are îndoieli sau i se aduc la cunoștință îndoieli cu privire la competența unui organism de evaluare a conformității de a îndeplini cerințele și responsabilitățile care îi revin sau la continuarea îndeplinirii acestora de către un organism de evaluare a conformității.

(2) Autoritatea națională de certificare a securității cibernetice prezintă Comisiei, la cerere, toate informațiile referitoare la temeiul notificării sau la menținerea competenței organismului de evaluare a conformității în cauză.

(3) Comisia se asigură că toate informațiile sensibile obținute pe parcursul investigațiilor sale sunt tratate în mod confidențial.

(4) În cazul în care constată că un organism de evaluare a conformității nu îndeplinește sau nu mai îndeplinește cerințele pentru a fi notificat, Comisia informează autoritatea națională de certificare a securității cibernetice în consecință și solicită acesteia să ia măsurile corective necesare, inclusiv anularea notificării, dacă este necesar.

(5) Statele membre se asigură că este disponibilă o cale de atac împotriva deciziilor organismelor notificate.

Articolul 95

Obligația de informare și de păstrare a informațiilor impusă organismelor de evaluare a conformității

(1) Organismele de evaluare a conformității informează autoritatea națională de certificare a securității cibernetice cu privire la următoarele:

(a) orice refuzare, restricționare, suspendare sau retragere a unui certificat;

(b) orice circumstanțe care afectează domeniul de aplicare și condițiile notificării menționate la articolul 93 alineatul (1);

(c) orice cerere de informare cu privire la activitățile de evaluare a conformității, primită de la autoritățile de supraveghere a pieței;

(d) la cerere, orice activitate de evaluare a conformității desfășurată în sfera notificării sale și orice alte activități desfășurate, inclusiv activități transfrontaliere și subcontractarea.

(2) Organismele de evaluare a conformității furnizează, de asemenea, ENISA informațiile menționate la alineatul (1) litera (a) pentru a facilita îndeplinirea sarcinilor care îi revin în temeiul articolului 79.

(3) Organismele de evaluare a conformității furnizează celorlalte organisme de evaluare a conformității în temeiul prezentului regulament care desfășoară activități similare de evaluare a conformității și care vizează aceleași produse TIC, servicii TIC, procese TIC, servicii de securitate gestionate sau entități a căror postură de securitate cibernetică este certificată, fără întârzieri nejustificate, informații relevante privind aspecte legate de rezultate negative și, la cerere, pozitive ale evaluării conformității.

(4) Organismele de evaluare a conformității țin un sistem de evidență care conține toate documentele și dovezile prezentate sau primite în legătură cu fiecare evaluare și certificare pe care o efectuează. Evidențele se stochează într-un mod securizat și accesibil pe perioada necesară în scopul certificării și timp de cel puțin cinci ani de la expirarea sau retragerea unui certificat european de securitate cibernetică relevant.

Secțiunea 3
Alte dispoziții

Articolul 96
Dreptul de a depune o plângere și dreptul la o cale de atac eficientă

(1) Persoanele fizice sau juridice au dreptul să depună o plângere la entitatea care a eliberat un certificat european de securitate cibernetică sau, dacă plângerea se referă la un certificat european de securitate cibernetică eliberat de un organism de evaluare a conformității în temeiul articolului 85 alineatul (4), la autoritatea națională relevantă de certificare a securității cibernetice.

(2) Autoritatea sau organismul la care s-a depus plângerea informează reclamantul despre evoluția procedurilor, despre decizia luată și despre dreptul de a exercita o cale de atac eficientă în temeiul alineatelor (3) și (4).

(3) În pofida oricăror căi de atac administrative sau a altor căi de atac fără caracter judiciar, persoanele fizice și juridice au dreptul să exercite o cale de atac eficientă cu privire la:

(a) deciziile luate de autoritatea sau organismul menționat la alineatul (1), inclusiv, după caz, în legătură cu emiterea necorespunzătoare, omisiunea de a emite sau recunoașterea unui certificat european de securitate cibernetică deținut de respectivele persoane fizice și juridice;

(b) omisiunea de a da curs unei plângeri depuse la o autoritate sau un organism menționat la alineatul (1).

(4) Acțiunile în temeiul prezentului articol se introduc în fața instanțelor din statul membru în care este situată autoritatea sau organismul împotriva căruia se exercită calea de atac.

Articolul 97
Sancțiuni

Statele membre stabilesc normele privind sancțiunile care se aplică în cazul încălcării prezentului titlu și al încălcării sistemelor europene de certificare a securității cibernetice și iau toate măsurile necesare pentru a asigura punerea în aplicare a acestor norme. Sancțiunile prevăzute trebuie să fie eficace, proporționale și disuasive. Statele membre informează Comisia fără întârziere cu privire la normele și măsurile respective și notifică acesteia orice modificare ulterioară care le afectează.

TITLUL IV
SECURITATEA LANȚURILOR DE APROVIZIONARE TIC

CAPITOLUL I
Cadrul privind lanțurile de aprovizionare TIC de încredere

Articolul 98
Domeniul de aplicare al cadrului

(1) Cadrul privind lanțurile de aprovizionare TIC de încredere prevede un mecanism de securitate la nivelul Uniunii pentru a aborda riscurile non-tehnice din sectoarele cu o importanță critică ridicată și din alte sectoare critice, astfel cum se menționează în Directiva (UE) 2022/2555. Mecanismul identifică activele TIC esențiale din lanțurile de aprovizionare TIC critice și stabilește măsuri de atenuare adecvate și proporționale cu privire la entitățile de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555.

(2) Obligațiile prevăzute în prezentul titlu nu aduc atingere obligațiilor prevăzute la articolul 13 din Regulamentul (UE) 2024/2847 și în dispozițiile naționale de transpunere a articolului 21 din Directiva (UE) 2022/2555.

(3) Dispozițiile prevăzute în prezentul capitol nu împiedică statele membre să adopte sau să mențină dispoziții care asigură un nivel mai ridicat de securitate cibernetică în lanțurile de aprovizionare TIC, cu condiția ca aceste dispoziții să fie în concordanță cu obligațiile care le revin în temeiul dreptului Uniunii.

Articolul 99
Evaluările riscurilor în materie de securitate

(1) Comisia sau un grup format din cel puțin trei state membre poate solicita grupului de cooperare instituit prin articolul 14 din Directiva (UE) 2022/2555 („Grupul de cooperare NIS”) să efectueze evaluări coordonate la nivelul Uniunii ale riscurilor în materie de securitate, în conformitate cu articolul 22 din directiva respectivă. În cazul în care se efectuează o evaluare a riscurilor în materie de securitate în urma unei astfel de cereri, aceasta trebuie să includă în special propunerea de identificare a activelor TIC esențiale ale lanțului de aprovizionare TIC respectiv, precum și a principalilor actori care generează amenințări, a riscurilor și a vulnerabilităților care afectează activele respective. Evaluările coordonate la nivelul Uniunii ale riscurilor în materie de securitate trebuie să elaboreze scenarii de risc și să propună măsuri de atenuare a riscurilor identificate.

(2) Evaluările coordonate la nivelul Uniunii ale riscurilor în materie de securitate se finalizează în termen de șase luni de la solicitarea menționată la alineatul (1). La cererea Comisiei, Grupul de cooperare NIS poate conveni asupra unei perioade mai scurte.

(3) În cazul în care Comisia are motive suficiente să considere că există o amenințare cibernetică semnificativă pentru securitatea Uniunii în legătură cu un lanț de aprovizionare TIC și că sunt necesare acțiuni pentru a menține buna funcționare a pieței interne, Comisia, fără întârziere:

(a) consultă statele membre cu privire la necesitatea de a lua una sau mai multe dintre măsurile de atenuare menționate la articolul 103 și

(b) efectuează o evaluare a riscurilor în materie de securitate, ținând seama de consultarea statelor membre. Evaluarea riscurilor în materie de securitate include identificarea propusă a activelor TIC esențiale, precum și a principalilor actori care generează amenințări, a riscurilor și a vulnerabilităților care afectează activele respective. Evaluarea riscurilor în materie de securitate trebuie să elaboreze scenarii de risc și să propună măsuri de atenuare a riscurilor identificate.

Articolul 100
Desemnarea țărilor terțe care prezintă motive de îngrijorare în materie de securitate cibernetică

(1) În cazul în care, ca urmare a evaluării riscurilor în materie de securitate menționate la articolul 99 sau pe baza altor surse, cum ar fi o declarație publică în numele Uniunii sau al unui stat membru, reiese că o țară terță prezintă un risc non-tehnic grav și structural pentru lanțurile de aprovizionare TIC, Comisia verifică riscul reprezentat de țara respectivă, ținând seama de următoarele elemente:

(a) existența în țara terță a unor legi care impun entităților aflate sub jurisdicția lor să raporteze autorităților din țara terță respectivă informații privind vulnerabilitățile software sau hardware înainte să se fi știut că vulnerabilitățile respective au fost exploatate;

(b) practicile existente în țara terță, demonstrate de surse independente, care impun entităților aflate sub jurisdicția țării terțe să raporteze autorităților din țara terță respectivă informații privind vulnerabilitățile software sau hardware înainte să se fi știut că vulnerabilitățile respective au fost exploatate;

(c) absența unor căi de atac eficace și a unor mecanisme de control independente și democratice care să poată corecta preocupările identificate în materie de securitate, inclusiv în ceea ce privește practicile existente menționate la litera (b);

(d) informații fundamentate cu privire la unul sau mai multe incidente ale unor actori care generează amenințări, care sunt controlați din țara respectivă și care își desfășoară activitatea în afara teritoriului țării respective și care desfășoară activități sau campanii cibernetice răuvoitoare, precum și lipsa capacității sau a voinței țării terțe de a coopera cu Comisia sau cu statele membre pentru a aborda riscul care decurge din funcționarea unor astfel de actori care generează amenințări;

(e) informațiile relevante care decurg din evaluările coordonate la nivelul Uniunii ale riscurilor în materie de securitate sau din rapoartele statelor membre sau ale organizațiilor internaționale.

(2) În cazul în care, în urma verificării menționate la alineatul (1), Comisia concluzionează că o țară terță prezintă riscuri non-tehnice grave și structurale pentru lanțurile de aprovizionare TIC, aceasta poate, prin intermediul unui act de punere în aplicare, să desemneze țara terță respectivă ca țară care prezintă motive de îngrijorare în materie de securitate cibernetică a lanțurilor de aprovizionare TIC. Acest act de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2).

(3) Comisia revizuiește periodic actele de punere în aplicare adoptate în conformitate cu alineatul (2).

(4) Furnizorii cu grad ridicat de risc nu au dreptul:

(a) să participe la elaborarea, evaluarea, consultarea sau luarea deciziilor privind standardele europene și documentele de standardizare europeană menționate la articolul 10 alineatul (1) din Regulamentul (UE) nr. 1025/2012 și specificațiile comune menționate la articolul 27 din Regulamentul (UE) 2024/2847 în domeniul securității cibernetice;

(b) să solicite sau să fie deținătorul oricărui certificat european de securitate cibernetică în temeiul titlului III;

(c) să devină organism acreditat de evaluare a conformității în temeiul titlului III;

(d) să solicite să devină furnizor autorizat al oricărui atestat european individual de competențe în materie de securitate cibernetică în temeiul titlului II secțiunea 4;

(e) să participe la procedurile de achiziții publice organizate în conformitate cu legislația de transpunere a Directivei 2014/24/UE și 2014/25/UE în ceea ce privește furnizarea de componente TIC sau de componente care includ componente TIC care urmează să fie utilizate în active TIC esențiale, astfel cum sunt identificate în conformitate cu articolul 102;

(f) să participe la orice activități din cadrul programelor și al instrumentelor de finanțare ale Uniunii puse în aplicare în cadrul gestiunii directe și indirecte în conformitate cu articolul 136 din Regulamentul (UE, Euratom) 2024/2509 și cu normele sectoriale ale Uniunii, precum și la orice activități de finanțare ale Uniunii puse în aplicare în cadrul gestiunii partajate în legătură cu furnizarea de componente TIC sau de componente care includ componente TIC care urmează să fie utilizate în active TIC esențiale identificate în conformitate cu articolul 102.

Autoritățile responsabile cu procedurile menționate la literele (a)-(f) efectuează evaluările necesare în sensul prezentului alineat. Autoritățile se pot baza, de asemenea, în acest scop, pe lista menționată la articolul 104.

(5) În cazurile în care un furnizor cu grad ridicat de risc a obținut deja un certificat european de securitate cibernetică în temeiul titlului III, autoritatea competentă îl retrage fără întârzieri nejustificate.

Articolul 101
Mecanismul general de securitate a lanțului de aprovizionare TIC

În cazul în care Grupul de cooperare NIS a efectuat o evaluare coordonată la nivelul Uniunii a riscurilor în materie de securitate în temeiul articolului 99 alineatul (1) din prezentul regulament sau după finalizarea procedurii în cazul unei amenințări cibernetice semnificative în temeiul articolului 99 alineatul (3) pentru un lanț de aprovizionare TIC, Comisia poate lua măsurile prevăzute la articolul 102 și la articolul 103 alineatele (1) și (2).

Articolul 102
Identificarea activelor TIC esențiale

(1) În cazul în care evaluarea riscurilor efectuată în conformitate cu articolul 99 alineatul (1) sau (3) indică riscuri semnificative în materie de securitate cibernetică în legătură cu un lanț de aprovizionare TIC, Comisia este împuternicită să adopte acte de punere în aplicare care identifică activele TIC esențiale utilizate pentru fabricarea de produse sau furnizarea de servicii de către entități de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2) din prezentul regulament.

(2) Atunci când identifică activele TIC esențiale menționate la alineatul (1), Comisia ia în considerare următoarele elemente:

(a) dacă activele respective au funcții esențiale și sensibile pentru funcționarea produselor fabricate sau a serviciilor furnizate de entitatea de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555;

(b) dacă incidentele, inclusiv cele cauzate de vulnerabilitățile exploatate legate de activele respective, pot conduce la perturbări grave ale lanțurilor de aprovizionare TIC pe piața internă sau la exfiltrarea datelor;

(c) dacă există o dependență de un număr limitat de furnizori ai activelor respective;

(d) rezultatele evaluării riscurilor menționate la articolul 99.

Articolul 103
Măsuri de atenuare în cadrul lanțului de aprovizionare TIC

(1) Comisia este împuternicită să adopte acte de punere în aplicare care stabilesc, atunci când este necesar pentru a asigura un nivel ridicat de securitate cibernetică, de reziliență cibernetică și de încredere în cadrul Uniunii, că respectivului tip specific de entități menționate în anexele I și II la Directiva (UE) 2022/2555 i se interzice să utilizeze, să instaleze sau să integreze în orice formă componente TIC sau componente TIC care includ componente TIC de la furnizori cu grad ridicat de risc, astfel cum sunt identificați în conformitate cu articolul 104, în activele TIC esențiale identificate în conformitate cu articolul 102. Astfel de acte de punere în aplicare prevăd perioade de tranziție adecvate, în cursul cărora Comisia publică lista furnizorilor cu grad ridicat de risc menționați la articolul 104, precum și perioade de timp suplimentare pentru eliminarea treptată a componentelor TIC și a componentelor TIC care includ componente TIC relevante. Un astfel de act de punere în aplicare poate specifica, de asemenea, aceste componente TIC sau componente care includ componente TIC.

(2) Comisia este împuternicită să adopte acte de punere în aplicare care stabilesc, atunci când este necesar pentru a asigura un nivel ridicat de securitate cibernetică, de reziliență cibernetică și de încredere în Uniune, că respectivul tip specific de entități menționate în anexele I și II la Directiva (UE) 2022/2555 fac obiectul uneia sau mai multora dintre următoarele măsuri de atenuare în ceea ce privește lanțul lor de aprovizionare TIC și, în special, activele TIC esențiale identificate în conformitate cu articolul 102, pentru a atenua riscurile identificate în evaluările riscurilor în materie de securitate efectuate în temeiul articolului 99:

(a) aplicarea cerințelor de transparență privind furnizarea de informații autorității competente cu privire la furnizorii din lanțul de aprovizionare TIC pentru activele TIC esențiale desemnate în conformitate cu articolul 102;

(b) interdicția legată de transferurile de date către țări terțe și de prelucrarea datelor la distanță dintr-o țară terță;

(c) măsurile tehnice care urmează să fie auditate de o parte terță, inclusiv:

(i) utilizarea prelucrării cu ajutorul unui dispozitiv;

(ii) segmentarea specifică a sistemelor de rețea;

(iii) dezactivarea oricărui acces de la distanță sau acces fizic la activele TIC esențiale;

(iv) dezactivarea caracteristicilor neesențiale;

(v) monitorizarea operațională a rețelei;

(vi) testarea hardware-ului și a software-ului.

(d) restricții legate de controlul operațional, inclusiv externalizarea funcțiilor organizaționale către furnizorii de servicii gestionate;

(e) restricții legate de relațiile contractuale ale entității cu furnizorii săi;

(f) cerința ca serviciul să fie operat, gestionat, întreținut sau sprijinit de personal aprobat de autoritățile naționale competente relevante;

(g) diversificarea ofertei de componente TIC sau de componente incluse în componentele TIC.

(3) La introducerea măsurilor menționate la alineatul (2), Comisia poate stabili cerințe tehnice și metodologice pentru aceste măsuri.

(4) Înainte de a adopta actele de punere în aplicare menționate la alineatele (1) și (2), Comisia evaluează riscurile și dependențele potențiale și, în special:

(a) după caz, nivelul de risc asociat utilizării, instalării sau integrării, sub orice formă, a componentelor TIC sau a componentelor care includ componente TIC de la furnizori cu grad ridicat de risc în active TIC esențiale;

(b) potențialele efecte asupra economiei și societății pe care obligația le poate avea asupra entităților de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555;

(c) disponibilitatea unor furnizori alternativi față de cei cu risc ridicat;

(d) potențiala perturbare a activităților economice și societale transfrontaliere cauzată de un incident care afectează lanțul de aprovizionare TIC al unei entități.

(5) Actele de punere în aplicare menționate la alineatele (1) și (2) de la prezentul articol se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2) și se revizuiesc cel puțin o dată la 36 de luni.

(6) În circumstanțe excepționale, care justifică o intervenție pentru a menține buna funcționare a pieței interne și în cazul în care Comisia are motive suficiente să considere că utilizarea, instalarea sau integrarea componentelor TIC sau a componentelor care includ componente TIC de la o anumită entitate stabilită într-o țară terță sau controlată de o țară terță sau de entități dintr-o țară terță sau de un resortisant al unei țări terțe reprezintă un risc non-tehnic semnificativ în materie de securitate cibernetică pentru activitățile economice sau societale din cel puțin trei state membre, Comisia consultă fără întârziere statele membre cu privire la necesitatea de a lua măsuri la nivelul Uniunii.

(7) Comisia este împuternicită să adopte acte de punere în aplicare pentru a stabili că unui anumit tip de entități menționate în anexele I și II la Directiva (UE) 2022/2555 i se interzice să utilizeze, să instaleze sau să integreze componente TIC sau componente care includ componente TIC de la o entitate menționată la alineatul (6). În acest scop, Comisia consultă entitățile de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555 care ar putea fi vizate de interdicție. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2). După caz, acestea includ perioade adecvate pentru eliminarea treptată a acestor componente TIC sau componente care includ

componente TIC. Un astfel de act de punere în aplicare poate specifica, de asemenea, aceste componente TIC sau componente care includ componente TIC care fac obiectul interdicției. Această interdicție vizează, de asemenea, componentele TIC sau componentele care includ componente TIC de la toate entitățile controlate de entitatea specifică menționată la alineatul (6).

(8) Actele de punere în aplicare menționate la alineatele (1), (2) și (7) pot preciza, de asemenea, că măsurile de atenuare sunt aplicabile numai tipurilor de entități menționate în anexele I și II la Directiva (UE) 2022/2555 de o anumită dimensiune.

(9) Articolul 100 alineatul (4) se aplică entității specifice stabilite într-o țară terță sau controlate de o țară terță sau de o entitate dintr-o țară terță sau de un resortisant al unei țări terțe menționat la alineatul (7).

(10) Actele de punere în aplicare adoptate în conformitate cu alineatele (1), (2) și (7) care sunt aplicabile tipurilor de entități menționate la punctul 10 din anexa I la Directiva (UE) 2022/2555 se aplică *mutatis mutandis* instituției, organelor, oficiilor și agențiilor europene.

Articolul 104
Identificarea furnizorilor cu grad ridicat de risc

(1) Prin intermediul unor acte de punere în aplicare, Comisia stabilește liste cu furnizorii cu grad ridicat de risc relevanți pentru interdicțiile prevăzute în actele de punere în aplicare adoptate în conformitate cu articolul 103 alineatul (1), cu articolul 103 alineatul (7) sau pentru interdicția menționată la articolul 111 alineatul (1).

(2) În acest scop, Comisia cartografiază furnizorii care furnizează componente TIC și componente care includ componente TIC relevante pentru interdicția menționată la alineatul (1).

Pe această bază, Comisia efectuează o evaluare inițială pentru a identifica care dintre furnizorii cartografiați ar putea fi stabiliți într-o țară terță desemnată în conformitate cu articolul 100 sau controlați de o astfel de țară terță, de o entitate stabilită într-o astfel de țară terță sau de un resortisant al unei astfel de țări terțe. De asemenea, Comisia realizează o cartografiere inițială a furnizorilor potențial controlați de entitatea menționată la articolul 103 alineatul (6).

(3) Comisia evaluează locul de stabilire, precum și structura de proprietate și de control a furnizorilor identificați inițial în conformitate cu alineatul (2) al doilea paragraf.

(4) În scopul evaluării menționate la alineatul (3), Comisia are dreptul de a solicita informațiile necesare de la furnizori. În cazul în care furnizorul nu furnizează informațiile necesare în termenul stabilit, Comisia poate concluziona că furnizorul este stabilit într-o țară terță desemnată în conformitate cu articolul 100 sau este controlat de o astfel de țară terță, de entități din țara terță respectivă sau de resortisanți ai țării terțe respective. În cazul în care Comisia efectuează o evaluare în sensul articolului 103 alineatul (7), iar furnizorul nu furnizează informațiile necesare în termenul stabilit, Comisia poate concluziona că furnizorul este controlat de o entitate desemnată în conformitate cu articolul respectiv. De asemenea, autoritățile competente menționate la articolul 112 fac schimb de informații relevante cu Comisia, la cerere.

(5) Comisia comunică furnizorului în cauză constatările preliminare privind evaluarea stabilirii, a controlului și a proprietății. Comisia acordă furnizorului posibilitatea de a fi audiat cu privire la aceste constatări preliminare.

(6) Comisia poate solicita unei autorități competente să efectueze evaluarea inițială privind stabilirea, proprietatea și controlul unui furnizor, în cazul în care acest lucru este justificat având în vedere caracteristicile activității furnizorului respectiv. O autoritate competentă se poate oferi să efectueze o astfel de evaluare inițială. Comisia verifică aceste constatări inițiale pentru a decide dacă furnizorul ar trebui inclus pe lista furnizorilor cu grad ridicat de risc.

(7) Comisia actualizează periodic lista furnizorilor cu grad ridicat de risc în vederea eliminării sau a adăugării de furnizori cu grad ridicat de risc. Furnizorii cu grad ridicat de risc incluși pe listă pot solicita Comisiei să reevalueze înființarea, controlul și structura de proprietate a acestora, pe baza furnizării de dovezi că au existat modificări relevante.

(8) În cazul în care o autoritate competentă constată, inclusiv pe baza informațiilor furnizate de o entitate de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555, că ar putea fi necesar ca un furnizor să fie inclus pe o listă a furnizorilor cu grad ridicat de risc, aceasta informează Comisia fără întârzieri nejustificate.

Articolul 105

Derogare pentru entitățile stabilite într-o țară terță sau controlate de entități dintr-o țară terță care prezintă motive de îngrijorare în materie de securitate cibernetică

(1) O entitate stabilită într-o țară terță sau controlată de entități dintr-o țară terță care prezintă motive de îngrijorare în materie de securitate cibernetică desemnate în conformitate cu articolul 100 poate adresa Comisiei o cerere motivată pentru derogare:

(a) de la a face obiectul interdicției impuse entităților de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555 de a utiliza, a instala sau a integra în orice formă componentele sale TIC sau componente care includ componentele sale TIC în activele TIC esențiale ale entităților respective, prin derogare de la articolul 111 sau de la actele de punere în aplicare adoptate în temeiul articolului 103 alineatul (1);

(b) de la a face obiectul interdicției de a participa la procedurile de achiziții publice organizate în conformitate cu legislația de transpunere a Directivei 2014/24/UE și a Directivei 2014/25/UE în ceea ce privește furnizarea de componente TIC sau de componente care includ componente TIC care urmează să fie utilizate în active TIC esențiale, astfel cum sunt definite în conformitate cu articolul 102, prin derogare de la articolul 100 alineatul (4).

(2) Cererea menționată la alineatul (1):

(a) precizează interesul entității stabilite într-o țară terță sau controlate de entități dintr-o țară terță care prezintă motive de îngrijorare în materie de securitate cibernetică desemnate în conformitate cu articolul 100 de a i se acorda derogarea menționată la alineatul (1) de la prezentul articol; și

(b) demonstrează cu dovezi clare că vor fi puse în aplicare măsuri de atenuare eficace pentru a aborda riscurile non-tehnice și pentru a asigura absența oricărei posibile exercitări a unor interferențe nejustificate din partea țării terțe

desemnate în temeiul articolului 100 în ceea ce privește furnizarea de componente TIC sau de componente care includ componente TIC pentru utilizarea, instalarea sau integrarea în activele TIC esențiale ale unei entități de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555.

(3) Comisia este împuternicită să adopte acte de punere în aplicare pentru a detalia condițiile menționate la alineatul (2) litera (b) și pentru a stabili norme detaliate cu privire la procedurile menționate la prezentul articol. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2).

(4) Comisia evaluează cererea menționată la alineatul (1) printr-un proces echitabil și transparent, ținând seama de:

(a) circumstanțele și elementele suplimentare menționate la articolul 100 alineatele (1) și (2) în legătură cu țara desemnată care prezintă motive de îngrijorare în materie de securitate cibernetică pentru lanțurile de aprovizionare TIC în care este stabilită entitatea sau din care este controlată;

(b) eficacitatea măsurilor de atenuare menționate la alineatul (2) litera (b);

(c) dacă derogarea acordată entității stabilite într-o țară terță sau controlate de entități dintr-o țară terță care prezintă motive de îngrijorare în materie de securitate cibernetică pentru lanțurile de aprovizionare TIC nu ar fi în detrimentul interesului Uniunii.

(5) În cazul în care, în urma evaluării prevăzute la alineatul (3), Comisia ajunge la concluzia că acordarea unei derogări este justificată, aceasta face acest lucru printr-o decizie, pe care o notifică solicitantului în termen de 9 luni de la primirea cererii.

(6) Atunci când adoptă o decizie menționată la alineatul (4), Comisia poate limita derogarea la o anumită perioadă de timp și poate supune derogarea unor condiții pentru entitate, inclusiv:

(a) un calendar pentru punerea în aplicare a măsurilor de atenuare menționate la alineatul (2) litera (b);

(b) audituri periodice efectuate de părți terțe pentru a asigura punerea în aplicare eficace a măsurilor de atenuare;

(c) obligațiile de raportare cu privire la conformitate.

(7) În cazul în care, în urma evaluării prevăzute la alineatul (3), Comisia ajunge la concluzia că nu se justifică acordarea unei derogări, aceasta face acest lucru printr-o decizie și o notifică solicitanților în termen de 9 luni de la primirea cererii.

(8) Din proprie inițiativă, Comisia poate să retragă sau să modifice decizia menționată la alineatul (4) în una sau mai multe dintre următoarele situații:

(a) a intervenit o schimbare substanțială cu privire la faptele pe care s-a fundamentat decizia;

(b) entitatea care a solicitat derogarea acționează contrar angajamentelor sale;

(c) derogarea s-a bazat pe informații incomplete, incorecte sau înșelătoare furnizate de entitatea solicitantă.

Articolul 106
Drepturi la apărare

Comisia se asigură că, înainte de a adopta un act de punere în aplicare în temeiul articolului 103 alineatul (7) sau înainte de a adopta o decizie de refuzare a acordării derogării în temeiul articolului 105 alineatul (7) pe baza unor elemente care nu au fost prezentate de solicitant sau înainte de a retrage o decizie în temeiul articolului 105 alineatul (8), entității în cauză i se oferă posibilitatea de a fi audiată, ținând seama de necesitatea, în unele cazuri, a unei proceduri de urgență.

Articolul 107
Registrul

Comisia ține un registru accesibil publicului cu deciziile sale menționate la articolul 105 alineatul (5). Registrul menționează numele entităților care au făcut obiectul unor astfel de decizii. Comisia actualizează registrul în mod regulat.

Articolul 108
Confidențialitate

Informațiile primite de Comisie în temeiul articolelor 105 și 106 se utilizează numai în scopul pentru care au fost obținute.

Articolul 109
Taxe

(1) Comisia percepe taxe pentru cererile depuse în conformitate cu articolul 105 alineatul (1).

(2) Taxele se exprimă și se plătesc în euro.

(3) Taxele trebuie să fie proporționale cu costurile legate de prelucrarea cererilor menționate la articolul 105 alineatul (1), de evaluarea criteriilor și a informațiilor menționate la articolul 105 alineatul (2) și de crearea, întreținerea și funcționarea registrului menționat la articolul 107. Toate cheltuielile Comisiei atribuite personalului implicat în aceste activități trebuie să fie incluse în aceste costuri.

(4) Comisia adoptă acte de punere în aplicare prin care stabilește norme detaliate privind taxele, precizând cuantumul taxelor și modalitatea de plată a acestora. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2).

CAPITOLUL II
Lanțurile de aprovizionare TIC în rețelele de comunicații electronice

Articolul 110
Activele TIC esențiale pentru rețelele de comunicații electronice mobile, fixe și prin satelit

(1) Activele TIC esențiale pentru rețelele de comunicații electronice mobile, fixe și prin satelit sunt cele prevăzute în anexa II.

(2) Componentele TIC sau componentele care includ componente TIC furnizate de furnizori cu grad ridicat de risc trebuie să fie eliminate treptat din activele TIC esențiale ale rețelelor de comunicații electronice mobile, fixe și prin satelit.

(3) Perioada de timp pentru eliminarea treptată a componentelor TIC sau a componentelor care includ componente TIC furnizate de furnizori cu grad ridicat de risc în ceea ce privește rețelele de comunicații electronice mobile nu trebuie să depășească 36 de luni de la publicarea listei furnizorilor cu grad ridicat de risc menționată la articolul 104, relevantă pentru rețelele de comunicații electronice mobile.

(4) Comisia este împuternicită să adopte acte de punere în aplicare în conformitate cu articolul 118 alineatul (2) pentru a specifica perioadele de timp pentru eliminarea treptată a componentelor TIC sau a componentelor care includ componente TIC furnizate de furnizori cu grad ridicat de risc în ceea ce privește rețelele de comunicații electronice fixe și prin satelit.

(5) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 119 pentru a modifica anexa II la prezentul regulament în vederea adaptării acesteia la evoluțiile tehnologice, ținând seama de elementele menționate la articolul 103 alineatul (4).

Articolul 111

Interdicții privind rețelele de comunicații electronice mobile, fixe și prin satelit

(1) Furnizorii de rețele de comunicații electronice mobile, fixe și prin satelit nu trebuie să utilizeze, să instaleze și să integreze, sub nicio formă, componente TIC sau componente care includ componente TIC de la furnizori cu grad ridicat de risc în exploatarea activelor TIC esențiale menționate în anexa II.

(2) În cazurile în care autoritatea competentă desemnată în temeiul prezentului regulament dintr-un stat membru diferă de autoritatea competentă în temeiul Regulamentului (UE) XX/XXXX [propunerea DNA], autoritatea competentă desemnată în temeiul prezentului regulament informează fără întârziere autoritatea competentă în temeiul Regulamentului (UE) XX/XXXX [propunerea DNA] cu privire la măsurile impuse furnizorilor de rețele de comunicații electronice mobile, fixe și prin satelit în conformitate cu articolul 114. Autoritățile asigură o cooperare strânsă în scopul supravegherii eficace și al asigurării respectării măsurilor respective.

CAPITOLUL III

Autoritățile competente, supravegherea și asigurarea respectării legislației, jurisdicția, dreptul la apărare

Articolul 112

Autoritățile competente

(1) Fiecare stat membru desemnează autoritățile competente menționate la articolul 8 din Directiva (UE) 2022/2555 ca autorități responsabile cu luarea măsurilor de supraveghere și de asigurare a respectării legislației menționate la articolul 114.

(2) Autoritățile competente sunt pe deplin imparțiale din punct de vedere structural și funcțional și nu sunt supuse niciunei influențe externe, directe sau indirecte; în special, acestea nu solicită și nici nu acceptă instrucțiuni de la nicio altă autoritate publică sau parte privată.

(3) Statele membre se asigură că autoritățile lor competente dispun de competențe adecvate, de resurse umane și tehnice suficiente și de expertiza relevantă pentru a pune în aplicare în mod eficace măsurile de supraveghere și de asigurare a respectării legislației menționate la articolul 114.

(4) Fiecare stat membru notifică Comisiei, fără întârzieri nejustificate, numele autorităților competente desemnate în conformitate cu alineatul (1), sarcinile respective ale acestor autorități și orice modificări ulterioare ale acestora. De asemenea, fiecare stat membru face publice denumirile autorităților competente desemnate în conformitate cu alineatul (1).

Articolul 113
Rețeaua pentru cooperare și servicii de sprijin a Comisiei

În vederea unei supravegheri eficace, Comisia instituie o rețea de cooperare a autorităților competente ale statelor membre menționate la articolul 112 și a Comisiei, care să servească drept platformă pentru cooperare și schimb de informații, în special în scopul evaluării stabilirii, controlului și proprietății menționate la articolul 104. Comisia oferă sprijin administrativ rețelei.

Articolul 114
Măsuri de supraveghere și de asigurare a respectării legislației

(1) Autoritățile competente menționate la articolul 112 au dreptul de a lua măsuri de supraveghere și de asigurare a respectării legislației în ceea ce privește entitățile de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555. Statele membre se asigură că măsurile menționate mai sus sunt efective, proporționale și cu efect de descurajare, ținând seama de circumstanțele fiecărui caz în parte. Statele membre notifică Comisiei normele adoptate în acest scop și modificările ulterioare ale acestora.

(2) Atunci când își exercită sarcinile de supraveghere în legătură cu entitățile menționate în anexele I și II la Directiva (UE) 2022/2555, autoritățile competente au dreptul de a supune entitățile respective următoarelor:

(a) unor cereri prin care se solicită o listă detaliată și actualizată a furnizorilor și prestatorilor lor de servicii relevanți;

(b) unor cereri de acces la datele, documentele și informațiile necesare pentru verificarea conformității cu prezentul regulament;

(c) unor inspecții la fața locului și unei supravegheri *ex situ*, inclusiv unor verificări aleatorii, realizate de profesioniști cu formare corespunzătoare;

(d) unor cereri privind compoziția produselor hardware sau software instalate sau integrate sub orice formă în rețea sau în sistem, inclusiv componentele și dependențele tranzitorii, într-un format utilizat în mod curent și care poate fi citit automat.

(3) Atunci când își exercită competențele de asigurare a respectării legislației în ceea ce privește entitățile de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555, autoritățile competente au dreptul:

(a) de a emite avertismente cu privire la încălcările prezentului regulament de către entitățile în cauză, prezentând faptele și considerațiile juridice relevante;

(b) de a adopta decizii prin care se impune entităților în cauză să remedieze încălcarea prezentului regulament sau deficiențele identificate în punerea în aplicare a măsurilor de atenuare;

(c) de a dispune ca entitățile în cauză să înceteze activitățile care încalcă prezentul regulament și să se abțină de la repetarea unor astfel de activități și

(d) de a impune sancțiuni, în conformitate cu normele referitoare la cuantumul prevăzut la articolul 115, sau de a solicita impunerea unor astfel de sancțiuni de către organismele, instanțele sau tribunalele relevante, în conformitate cu dreptul intern.

(4) Atunci când iau oricare dintre măsurile de asigurare a respectării legislației menționate la alineatul anterior, autoritățile competente iau în considerare circumstanțele fiecărui caz în parte și țin seama în mod corespunzător de următorii factori:

(a) gravitatea încălcării și importanța dispozițiilor încălcate;

(b) durata încălcării;

(c) cifra de afaceri relevantă a entității în cauză;

(d) orice încălcare anterioară relevantă comisă de entitatea în cauză;

(e) după caz, orice prejudiciu material sau moral cauzat de încălcare, inclusiv orice pierdere financiară sau economică, efectele asupra altor entități și numărul de utilizatori afectați;

(f) orice intenție sau neglijență din partea entității în cauză;

(g) orice măsuri luate de entitate pentru a preveni sau a atenua prejudiciile materiale sau morale;

(h) nivelul de cooperare cu autoritățile competente al persoanelor fizice sau juridice considerate responsabile.

În sensul primului paragraf litera (a), constituie încălcări grave următoarele:

(i) încălcări repetate;

(j) neîndeplinirea obligației de notificare sau de remediere a incidentelor semnificative;

(k) neremedierea deficiențelor în urma instrucțiunilor obligatorii din partea autorităților competente

(5) Autoritățile competente notifică entităților în cauză constatările lor preliminare înainte de a lua măsuri de asigurare a respectării legislației. Entităților în cauză li se acordă un termen rezonabil pentru a prezenta observații cu privire la constatările preliminare. Autoritățile competente prezintă o motivare detaliată a măsurilor lor de asigurare a respectării legislației.

(6) Autoritățile competente respectă principiile confidențialității și secretului profesional și comercial.

(7) Autoritățile competente cooperează între ele și cu Comisia în scopul supravegherii și al asigurării respectării legislației în temeiul prezentului titlu, în conformitate cu articolul 116.

Articolul 115
Sancțiuni

(1) Statele membre adoptă normele privind sancțiunile care se aplică în cazul nerespectării prezentului regulament și iau toate măsurile necesare pentru a asigura aplicarea acestora.

(2) Sancțiunile prevăzute trebuie să fie eficace, proporționale și disuasive. Statele membre notifică normele respective Comisiei și îi comunică acesteia, fără întârziere, orice modificări ulterioare privind aceste norme.

(3) Se impun sancțiuni în plus față de oricare dintre măsurile menționate la articolul 114 alineatul (3) literele (a), (b) și (c).

(4) Atunci când se decide dacă să se impună o sancțiune și se decide cuantumul acesteia în fiecare caz în parte, se acordă atenția cuvenită cel puțin factorilor menționați la articolul 114 alineatul (4) primul paragraf.

(5) În conformitate cu alineatul (3) de la prezentul articol, încălcările articolului 103 alineatul (2) litera (a) fac obiectul unor sancțiuni de maximum 1 % din cifra de afaceri mondială totală anuală din exercițiul financiar precedent a întreprinderii căreia îi aparține entitatea.

(6) În conformitate cu alineatul (3) de la prezentul articol, încălcările articolului 103 alineatul (2) literele (b)-(g) fac obiectul unor sancțiuni de maximum 2 % din cifra de afaceri mondială totală anuală din exercițiul financiar precedent a întreprinderii căreia îi aparține entitatea.

(7) În conformitate cu alineatul (3) de la prezentul articol, încălcările articolului 103 alineatul (1) și ale articolului 111 fac obiectul unor sancțiuni de maximum 7 % din cifra de afaceri mondială totală anuală din exercițiul financiar precedent a întreprinderii căreia îi aparține entitatea.

Articolul 116
Asistența reciprocă

(1) În cazul în care o entitate de tipul celor menționate în anexele I sau II la Directiva (UE) 2022/2555 furnizează servicii în mai multe state membre sau furnizează servicii în unul sau mai multe state membre, iar activele sale TIC esențiale sunt situate în unul sau mai multe alte state membre, autoritățile competente ale statelor membre în cauză cooperează între ele și cu Comisia și își acordă reciproc asistență și acordă asistență Comisiei, în vederea asigurării aplicării eficace și eficiente a regulamentului. În acest scop, se aplică cel puțin următoarele norme:

(a) autoritățile competente care aplică măsuri de supraveghere sau de asigurare a respectării legislației într-un stat membru informează și consultă autoritățile competente din celelalte state membre în cauză cu privire la măsurile de supraveghere și de asigurare a respectării legislației luate;

(b) o autoritate competentă dintr-un stat membru poate solicita unei alte autorități competente dintr-un alt stat membru să ia măsuri de supraveghere sau de asigurare a respectării legislației;

(c) la primirea unei cereri motivate din partea unei alte autorități competente dintr-un alt stat membru, o autoritate competentă dintr-un stat membru acordă asistență reciprocă celeilalte autorități competente, depunând toate eforturile,

astfel încât măsurile de supraveghere sau de asigurare a respectării legislației să poată fi puse în aplicare în mod eficace, eficient și consecvent.

(2) Asistența reciprocă menționată la alineatul (1) litera (c) poate acoperi cererile de informații și măsurile de supraveghere, inclusiv cererile de efectuare a unor inspecții la fața locului, a unei supravegheri *ex situ* sau a unor audituri de securitate specifice. O autoritate competentă căreia i se adresează o cerere de asistență nu refuză cererea respectivă, cu excepția cazului în care se stabilește că nu are competența de a furniza asistența solicitată, asistența solicitată nu este proporțională cu sarcinile de supraveghere ale autorității competente sau cererea privește informații sau implică activități care, dacă ar fi divulgate sau desfășurate, ar fi contrare intereselor esențiale ale statului membru respectiv în materie de securitate națională, siguranță publică sau apărare. Înainte de a refuza o astfel de cerere, autoritatea competentă consultă celelalte autorități competente în cauză, precum și, la cererea unuia dintre statele membre în cauză, Comisia.

(3) Dacă este cazul și de comun acord, autorități competente din diferite state membre pot desfășura acțiuni comune de supraveghere.

(4) Având în vedere obligația de a respecta principiile confidențialității și secretului profesional și comercial, astfel cum se menționează la articolul 114 alineatul (6), orice informații comunicate în contextul unei cereri de asistență și furnizate în temeiul prezentului articol se utilizează numai în scopul pentru care au fost solicitate.

Articolul 117
Jurisdicție și teritorialitate

(1) Se consideră că entitățile de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555 care intră în domeniul de aplicare al prezentului regulament intră sub jurisdicția statului membru în care sunt stabilite, cu următoarele excepții:

(a) furnizorii de rețele publice de comunicații electronice sau furnizorii de servicii de comunicații electronice accesibile publicului, care se consideră că intră sub jurisdicția statului membru în care își prestează serviciile;

(b) furnizorii de servicii DNS, registrele de nume de domenii de prim nivel (TLD), furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, precum și furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, care se consideră că se află sub jurisdicția statului membru în care își au sediul principal în Uniune în temeiul alineatului (2);

(c) entitățile administrației publice, care se consideră că intră sub jurisdicția statului membru căruia îi aparțin;

(d) transportatorii aerieni, în privința cărora se consideră că se află sub jurisdicția statului membru a cărui autoritate competentă pentru acordarea licențelor a acordat licența de operare entității în temeiul Regulamentului (CE) nr. 1008/2008 al Parlamentului European și al Consiliului[83] sau, în cazul în

[83] Regulamentul (CE) nr. 1008/2008 al Parlamentului European și al Consiliului din 24 septembrie 2008 privind normele comune pentru operarea serviciilor aeriene în Comunitate (reformare) (JO L 293, 31.10.2008, p. 3, ELI: https://eur-lex.europa.eu/eli/reg/2008/1008/oj/eng).

care licența de operare sau echivalentul acesteia nu a fost acordat(ă) în conformitate cu regulamentul respectiv, se află sub jurisdicția statului membru în care își au sediul principal în Uniune în temeiul alineatului (2).

(2) În sensul prezentului regulament, se consideră că o entitate, astfel cum este menționată la alineatul (1) litera (b), își are sediul principal din Uniune în statul membru în care se iau în mod predominant deciziile legate de măsurile de gestionare a riscurilor în materie de securitate cibernetică. Dacă un astfel de stat membru nu poate fi stabilit sau dacă astfel de decizii nu sunt luate în Uniune, sediul principal este considerat a fi în statul membru în care se desfășoară majoritatea operațiunilor de securitate cibernetică. Dacă un astfel de stat membru nu poate fi stabilit, sediul principal este considerat a fi în statul membru în care entitatea în cauză își are sediul cu cel mai mare număr de angajați din Uniune.

(3) Dacă o entitate de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555 nu este stabilită în Uniune, dar oferă servicii în Uniune, aceasta trebuie să desemneze un reprezentant în Uniune. Reprezentantul se stabilește în unul dintre statele membre în care se oferă serviciile. O astfel de entitate se consideră a fi sub jurisdicția statului membru în care este stabilit reprezentantul. În cazul în care o astfel de entitate este o entitate menționată la alineatul (1) litera (a), se consideră că aceasta se află sub jurisdicția statului membru în care își prestează serviciile. În absența unui reprezentant în Uniune desemnat în temeiul prezentului alineat, orice stat membru în care entitatea prestează servicii poate introduce acțiuni în justiție împotriva entității pentru încălcarea prezentului regulament.

(4) Desemnarea unui reprezentant de către o entitate menționată la alineatul (1) litera (b) nu aduce atingere acțiunilor în justiție care ar putea fi inițiate împotriva entității înseși.

(5) Statele membre care au primit o cerere de asistență reciprocă în legătură cu o entitate, astfel cum este menționată la alineatul (1) litera (b), pot, în limitele cererii respective, să ia măsuri adecvate de supraveghere și de asigurare a respectării legii în ceea ce privește entitatea în cauză în cazul în care entitatea furnizează servicii sau are o rețea și un sistem informatic pe teritoriul lor.

TITLUL VI
DISPOZIȚII FINALE

Articolul 118
Procedura comitetului

(1) Comisia este asistată de un comitet. Acest comitet are două configurații. În ceea ce privește titlurile II și III, Comisia este asistată de un comitet în prima configurație, în timp ce în ceea ce privește titlul IV, Comisia este asistată de un comitet în a doua configurație. Respectivul comitet reprezintă un comitet în înțelesul Regulamentului (UE) nr. 182/2011.

(2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

Articolul 119
Exercitarea delegării de competențe

(1) Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol.

(2) Competența de a adopta acte delegate în conformitate cu articolul 80 alineatul (2) și cu articolul 110 alineatul (5) se conferă Comisiei pe o perioadă nedeterminată de la data intrării în vigoare a prezentului regulament.

(3) Delegarea de competențe menționată la articolul 80 alineatul (2) și la articolul 110 alineatul (5) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării acesteia în *Jurnalul Oficial al Uniunii Europene* sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.

(4) Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare.

(5) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

(6) Un act delegat adoptat în temeiul articolului 80 alineatul (2) și al articolului 110 alineatul (5) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 120
Evaluare și revizuire

(1) Până la [ZZ LL AAAA] și, ulterior, o dată la cinci ani, Comisia comandă o evaluare care se efectuează în conformitate cu orientările Comisiei.

(2) Evaluarea menționată la alineatul (1) include o analiză a următoarelor elemente:

(a) performanța ENISA în raport cu obiectivele, mandatul, misiunea, sarcinile, guvernanța și localizarea acesteia;

(b) eficacitatea, eficiența și valoarea adăugată europeană a sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică, astfel cum se prevede în titlul II capitolul II secțiunea 4 din prezentul regulament;

(c) impactul, eficacitatea și eficiența dispozițiilor din titlul III din prezentul regulament în ceea ce privește obiectivele de asigurare a unui nivel adecvat de securitate cibernetică a produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate și a entităților în Uniune și de îmbunătățire a funcționării pieței interne;

(d) impactul, eficacitatea și eficiența dispozițiilor titlului IV din prezentul regulament în ceea ce privește obiectivele cadrului privind lanțul de aprovizionare TIC de încredere.

(3) Evaluarea menționată la alineatul (1) litera (a) abordează, în special, posibila necesitate de a modifica mandatul ENISA, precum și implicațiile financiare ale unei astfel de modificări.

(4) La fiecare a doua evaluare menționată la alineatul (1) litera (a), Comisia evaluează rezultatele obținute de ENISA având în vedere obiectivele, mandatul, misiunea, guvernanța și sarcinile sale, inclusiv o evaluare a măsurii în care continuarea activității ENISA este în continuare justificată în ceea ce privește obiectivele, mandatul, misiunea, guvernanța și sarcinile respective.

(5) Comisia prezintă Parlamentului European, Consiliului și consiliului de administrație un raport privind concluziile evaluării. Rezultatele evaluării se fac publice.

Articolul 121
Abrogarea și continuarea activităților

(1) Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului se abrogă de la ZZLLAAAA.

(2) Trimiterile la Regulamentul (UE) 2019/881, la ENISA și la sistemele europene de certificare a securității cibernetice instituite prin regulamentul respectiv se interpretează ca trimiteri la prezentul regulament și se citesc în conformitate cu tabelul de corespondență din anexa III la prezentul regulament.

(3) ENISA, astfel cum este reglementată de prezentul regulament, continuă operațiunile și activitățile ENISA, astfel cum a fost instituită prin Regulamentul (UE) 2019/881, în ceea ce privește toate aspectele legate de proprietate, acorduri, obligații legale, contracte de muncă, angajamente financiare și răspunderi. Toate deciziile consiliului de administrație și ale comitetului executiv adoptate cu conformitate cu Regulamentul (UE) 2019/881 rămân valabile, cu condiția ca acestea să respecte prezentul regulament.

(4) Directorul executiv numit în temeiul articolului 15 alineatul (1) litera (n) din Regulamentul (UE) 2019/881 rămâne în funcție și exercită sarcinile și responsabilitățile directorului executiv, astfel cum se menționează la articolul 32 din prezentul regulament, pentru perioada rămasă din mandatul directorului executiv. Celelalte condiții ale contractului său rămân neschimbate.

(5) Se consideră că proiectele de sisteme a căror pregătire a fost solicitată în temeiul articolului 49 din Regulamentul (UE) 2019/881 au fost solicitate în conformitate cu dispozițiile corespunzătoare din prezentul regulament. Dispozițiile titlului III din prezentul regulament se aplică în mod corespunzător respectivelor propuneri de sisteme.

(6) Membrii consiliului de administrație numiți de Comisie și membrii supleanți numiți în temeiul articolului 14 din Regulamentul (UE) 2019/881 rămân în funcție și exercită funcțiile consiliului de administrație, astfel cum se menționează la articolul 27 din prezentul regulament, pentru perioada rămasă din mandatul lor. Membrii consiliului de administrație numiți de statele membre în temeiul articolului 14 din Regulamentul (UE) 2019/881 rămân în funcție și exercită funcțiile consiliului de administrație, astfel cum se menționează la articolul 27 din prezentul regulament, cu condiția să dețină funcțiile menționate la articolul 24 alineatul (3) din prezentul regulament.

Articolul 122
Intrarea în vigoare

Prezentul regulament intră în vigoare în a […] zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Strasbourg,

Pentru Parlamentul European,	*Pentru Consiliu,*
Președinta	*Președintele*

FIȘĂ FINANCIARĂ LEGISLATIVĂ ȘI DIGITALĂ

1. CADRUL PROPUNERII/INIȚIATIVEI ... 3
1.1. Titlul propunerii/inițiativei ... 3
1.2. Domeniul (domeniile) de politică vizat(e) ... 3
1.3. Obiectiv(e) ... 3
1.3.1. Obiectiv(e) general(e) ... 3
1.3.2. Obiectiv(e) specific(e) ... 3
1.3.3. Rezultatul (rezultatele) și impactul preconizate ... 3
1.3.4. Indicatori de performanță ... 3
1.4. Obiectul propunerii/inițiativei ... 4
1.5. Motivele propunerii/inițiativei ... 4
1.5.1. Cerința (cerințele) care trebuie îndeplinită (îndeplinite) pe termen scurt sau lung, inclusiv un calendar detaliat pentru punerea în aplicare a inițiativei ... 4
1.5.2. Valoarea adăugată a intervenției UE (aceasta poate rezulta din diferiți factori, de exemplu mai buna coordonare, securitatea juridică, o mai mare eficacitate sau complementaritate). În sensul prezentei secțiuni, „valoarea adăugată a intervenției UE” este valoarea ce rezultă din acțiunea UE care depășește valoarea ce ar fi fost obținută dacă ar fi acționat doar statele membre. ... 4
1.5.3. Învățăminte desprinse din experiențele anterioare similare ... 4
1.5.4. Compatibilitatea cu cadrul financiar multianual și posibilele sinergii cu alte instrumente corespunzătoare ... 5
1.5.5. Evaluarea diverselor opțiuni de finanțare disponibile, inclusiv a posibilităților de realocare a creditelor ... 5
1.6. Durata propunerii/inițiativei și a impactului său financiar ... 6
1.7. Metoda (metodele) de execuție a bugetului planificată (planificate) ... 6
2. MĂSURI DE GESTIUNE ... 8
2.1. Dispoziții în materie de monitorizare și de raportare ... 8
2.2. Sistemul (sistemele) de gestiune și de control ... 8
2.2.1. Justificarea metodei (metodelor) de execuție bugetară, a mecanismului (mecanismelor) de punere în aplicare a finanțării, a modalităților de plată și a strategiei de control propuse ... 8
2.2.2. Informații privind riscurile identificate și sistemul (sistemele) de control intern instituit(e) pentru atenuarea lor ... 8
2.2.3. Estimarea și justificarea raportului cost-eficacitate al controalelor (raportul dintre costurile controalelor și valoarea fondurilor aferente gestionate) și evaluarea nivelurilor estimate ale riscurilor de eroare (la plată și la închidere) ... 8
2.3. Măsuri de prevenire a fraudelor și a neregulilor ... 9
3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI ... 10

3.1. Rubrica (rubricile) din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate) 10
3.2. Impactul financiar estimat al propunerii asupra creditelor 12
3.2.1. Sinteza impactului estimat asupra creditelor operaționale 12
3.2.1.1. Credite din bugetul votat 12
3.2.1.2. Credite din venituri alocate externe 17
3.2.2. Realizările preconizate finanțate din credite operaționale 22
3.2.3. Sinteza impactului estimat asupra creditelor administrative 24
3.2.3.1. Credite din bugetul votat 24
3.2.3.2. Credite din venituri alocate externe 24
3.2.3.3. Total credite 24
3.2.4. Necesarul de resurse umane estimat 25
3.2.4.1. Finanțare din bugetul votat 25
3.2.4.2. Finanțare din venituri alocate externe 26
3.2.4.3. Necesarul total de resurse umane 26
3.2.5. Prezentare generală a impactului estimat asupra investițiilor legate de tehnologia digitală 28
3.2.6. Compatibilitatea cu cadrul financiar multianual actual 28
3.2.7. Contribuțiile terților 28
3.3. Impactul estimat asupra veniturilor 29
4. DIMENSIUNILE DIGITALE 29
4.1. Cerințe cu relevanță digitală 30
4.2. Date 30
4.3. Soluții digitale 31
4.4. Evaluarea interoperabilității 31
4.5. Măsuri de sprijinire a implementării digitale 32

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Titlul propunerii/inițiativei

Propunere de regulament al Parlamentului European și al Consiliului privind Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), cadrul european de certificare a securității cibernetice și securitatea lanțului de aprovizionare TIC și de abrogare a Regulamentului (UE) 2019/881 (Regulamentul privind securitatea cibernetică 2)

(Text cu relevanță pentru SEE)

Titlu scurt: Regulamentul privind securitatea cibernetică 2 (CSA2)

și

Propunere de directivă a Parlamentului European și a Consiliului de modificare a Directivei (UE) 2022/2555 în ceea ce privește măsurile de simplificare și alinierea la [Propunerea de regulament privind securitatea cibernetică 2]

1.2. Domeniul (domeniile) de politică vizat(e)

Domeniul de politică: 09 - Rețele de comunicații, conținut și tehnologie

Activitate: 09.02 piața unică digitală

1.3. Obiectiv(e)

1.3.1. Obiectiv(e) general(e)

Principalele obiective ale intervenției sunt:

(1) Consolidarea capacităților și a rezilienței în materie de securitate cibernetică

Contribuția la consolidarea guvernanței Uniunii în materie de securitate cibernetică și la asigurarea faptului că instituțiile, autoritățile și alte părți interesate relevante sunt mai bine pregătite pentru a preveni, a detecta amenințările la adresa securității cibernetice și a răspunde la acestea într-un mod coordonat și eficace.

(2) Prevenirea fragmentării pe piața internă prin:

Sprijinirea dezvoltării, a punerii în aplicare și a adoptării unor instrumente comune ale Uniunii în materie de securitate cibernetică, cum ar fi sistemele de certificare, și furnizarea unor cadre armonizate care să consolideze încrederea și interoperabilitatea în toate statele membre.

Aceste obiective generale răspund principalelor provocări identificate în definirea problemei din evaluarea impactului inițiativei propuse. Acestea reflectă obiectivul general de politică de consolidare a guvernanței în materie de securitate cibernetică în Uniune și de sprijinire a dezvoltării unei piețe unice digitale sigure, reziliente și competitive.

1.3.2. Obiectiv(e) specific(e)

Pentru a aborda neconcordanța dintre cadrul de politică al UE în materie de securitate cibernetică și nevoile părților interesate:

Obiectivul specific nr. 1: Crearea capacității de a pune în aplicare în mod eficace politicile Uniunii în materie de securitate cibernetică și cooperarea operațională continuă care să permită o cooperare mai structurată între statele membre.

Obiectivul specific nr. 2: Dezvoltarea și punerea în aplicare a unor mijloace și mecanisme pentru a sprijini și a aborda în mod eficace nevoile statelor membre, ale industriei și ale altor părți interesate.

Pentru a aborda gradul limitat de adoptare și eficacitatea limitată ale Cadrului european de certificare a securității cibernetice (ECCF):

Obiectivul specific nr. 3: Crearea condițiilor prealabile pentru furnizarea mai rapidă a sistemelor de certificare a securității cibernetice determinate de nevoile pieței prin extinderea domeniului de aplicare al ECCF, prin asigurarea unei întrețineri eficace și a unor proceduri flexibile și prin creșterea transparenței.

Pentru a aborda peisajul fragmentat al conformității și complexitatea cadrelor orizontale și sectoriale:

Obiectivul specific nr. 4: Crearea de mecanisme și condiții pentru a facilita respectarea cerințelor de securitate cibernetică, făcând astfel punerea lor în aplicare mai coerentă și mai eficace.

Pentru a aborda riscurile în materie de securitate cibernetică de la nivelul lanțurilor de aprovizionare:

Obiectivul specific nr. 5: Reducerea riscurilor de la nivelul lanțurilor de aprovizionare TIC critice de la entități stabilite în țări sau controlate de entități din țări care prezintă motive de îngrijorare în materie de securitate cibernetică (furnizori cu grad ridicat de risc) și reducerea dependențelor critice prin dezvoltarea unui cadru coerent și eficace la nivelul UE pentru a aborda riscurile la adresa securității lanțurilor de aprovizionare TIC.

1.3.3. Rezultatul (rezultatele) și impactul preconizate

A se preciza efectele pe care ar trebui să le aibă propunerea/inițiativa asupra beneficiarilor vizați/grupurilor vizate.

Rezultatele preconizate sunt următoarele:

(1) Reforma funcțională a ENISA

(2) Reforma ECCF – extinderea domeniului de aplicare, o nouă procedură și guvernanță revizuită

(3) Simplificarea în continuare a respectării cadrului legislativ relevant al Uniunii în materie de securitate cibernetică

(4) Un cadru cuprinzător și orizontal pentru abordarea riscurilor în materie de securitate cibernetică de la nivelul lanțurilor de aprovizionare TIC

Impactul global:

Propunerea va avea un impact imens asupra securității cibernetice în Uniune, deoarece abordează o serie de domenii, cum ar fi consolidarea necesară a Agenției Uniunii Europene pentru Securitate Cibernetică, consolidează sprijinul pentru punerea în aplicare a legislației UE, introduce reforme pentru punerea în aplicare fără probleme a cadrului european de certificare, sprijină înțelegerea comună de către Uniune a amenințărilor cibernetice și abordează atenuarea riscurilor în materie de securitate cibernetică în funcție de realitatea geopolitică. Punerea în aplicare a dispozițiilor propuse va asigura niveluri ridicate de eficiență și coerență și va evita o sarcină de reglementare excesivă. Pachetul este conceput pentru a fi rezilient la provocările legate de punerea în aplicare și pentru a sprijini coerența politicilor pe

termen lung în întregul ecosistem digital și de securitate cibernetică. Acesta îmbunătățește claritatea, eliminând ineficiențele și aliniind procedurile între cadrele juridice, contribuind în același timp la atingerea unui nivel ridicat de securitate cibernetică în întreaga UE. Fiind unul dintre principalele obiective prioritare ale Comisiei Europene, eforturile de simplificare avute în vedere vor aduce beneficii economice semnificative întreprinderilor, inclusiv IMM-urilor, în valoare de peste 14,63 miliarde EUR, iar autorităților publice, în valoare de 7,5 milioane EUR.

Printre rezultatele specifice se numără:

- creșterea gradului de conștientizare și îmbunătățirea coordonării operaționale, care ar putea genera economii considerabile de costuri legate de detectarea mai rapidă a incidentelor și de răspunsul mai rapid la acestea pentru întreprinderi, autoritățile publice și cetățeni;
- asigurarea clarității domeniului de aplicare și a mandatului ENISA, asigurând, în același timp, definire necesară a priorităților în privința sarcinilor sale principale;
- asigurarea faptului că părțile interesate primesc sprijin adecvat pentru punerea în aplicare a politicilor, pentru activitățile operaționale și pentru coordonarea generală;
- Sprijinirea conștientizării comune a situației de către Uniune
- cooperarea consolidată cu EU-CyCLONe, rețeaua CSIRT, Comisia, Europol și CERT-UE și cu entitățile relevante ale Uniunii, cu scopul de a crea registre de informații verificate și fiabile privind amenințările cibernetice;
- sprijinirea eforturilor de atenuare a atacurilor de tip ransomware;
- o mai bună coordonare cu sectorul privat pe teme legate de securitatea cibernetică;
- difuzarea în timp util de informații prin alerte timpurii privind un incident semnificativ sau de mare amploare sau o amenințare cibernetică de natură transfrontalieră, în legătură cu sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555;
- promovarea de sinergii eficace cu alte organisme și agenții ale UE;
- reducerea prețului certificărilor competențelor, inclusiv prin creșterea ofertei pe piață prin introducerea sistemelor europene de atestare a competențelor;
- sprijinirea eliminării lacunelor în materie de competențe din Europa prin atestări individuale ale competențelor în materie de securitate cibernetică și sprijinirea statelor membre și a industriei în consolidarea forței lor de muncă;
- abordarea lipsei de claritate a cadrului ECCF și a impactului său limitat, extinderea domeniului său de aplicare și îmbunătățirea modelului său de guvernanță;
- creșterea reputației sistemelor adoptate prin instituirea unei structuri de întreținere și prin introducerea unui proces de dezvoltare transparent și în timp util;
- introducerea unui mecanism de taxe în legătură cu costurile care apar pentru dezvoltarea și menținerea sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică și pentru prelucrarea

cererilor și acordarea de autorizații furnizorilor, precum și pentru întreținerea sistemelor, adoptat în cadrul ECCF, care va contribui la stabilitatea financiară a agenției și va crea economii la bugetul UE;

- alinierea sistemelor europene de certificare la cadrul legislativ existent și, prin urmare, o mai bună sprijinire a eforturilor de punere în aplicare și a nevoilor de conformitate ale întreprinderilor;
- facilitarea adoptării sistemelor blocate în prezent;
- stimularea competitivității întreprinderilor europene prin promovarea alinierii între standardele internaționale și cele europene;
- limitarea fragmentării măsurilor și cerințelor de securitate cibernetică;
- asigurarea clarității juridice și reducerea substanțială a sarcinii administrative, fără a conduce la o incertitudine juridică semnificativă în rândul părților interesate care sunt în curs de adaptare la cadrele juridice recent adoptate;
- facilitarea conformității pentru entitățile NIS2, ceea ce ar contribui, de asemenea, la o mai bună rată de conformitate în general și la instituirea unor măsuri de securitate cibernetică mai semnificative, eficientizând în același timp procesul de supraveghere din partea autorităților;

Altele

- IMM-urile ar beneficia de numeroase efecte pozitive ale inițiativei, având în vedere îmbunătățirea competitivității pe piața securității cibernetice a UE, precum și reducerea costurilor și a sarcinii administrative:

1. *Un rol pozitiv pentru IMM-uri, care ar beneficia de o reziliență cibernetică sporită datorită unui rol sporit al ENISA și orientărilor tehnice furnizate de agenție.*
2. *IMM-urile, în calitate de furnizor autorizat să emită atestate în cadrul sistemului european de atestare a competențelor, vor câștiga vizibilitate, reputație și clienți. În plus, atestatele europene individuale de competențe în materie de securitate cibernetică vor sprijini IMM-urile să identifice candidații cu setul de competențe adecvat.*
3. *Buna funcționare a sistemelor europene de certificare poate facilita alegerea tehnologiilor TIC de încredere pentru IMM-uri și poate contribui la consolidarea rezilienței cibernetice generale a acestora.*
4. *În calitate de furnizori DNS, IMM-urile vor beneficia de măsuri legate de punerea în aplicare a Directivei NIS2 din cauza excluderilor din domeniul de aplicare al furnizorilor DNS.*
5. *IMM-urile ar beneficia de pe urma clarificărilor privind domeniul de aplicare care ar limita aplicarea obligațiilor la anumite entități din unele sectoare enumerate în Directiva NIS 2.*
6. *În ceea ce privește măsurile de securitate a lanțului de aprovizionare TIC, IMM-urile, în general, ar beneficia de pe urma utilizării tehnologiilor de încredere. În calitate de furnizori activi în sectoarele care fac obiectul restricțiilor, aceștia ar fi afectați mai puternic de costurile de substituție și de tranzacție în comparație cu întreprinderile mai mari. Cu toate acestea, IMM-urile, în calitate de furnizori de încredere, vor beneficia de noi oportunități de piață.*

- nu se preconizează un impact de mediu semnificativ pentru niciunul dintre obiective.

- în ceea ce privește bugetul UE, există posibilitatea sporirii eficienței prin intensificarea cooperării și a coordonării activităților între instituțiile, agențiile și organele UE. Se preconizează realizarea de economii pe termen lung prin introducerea unor mecanisme de taxare.

1.3.4. Indicatori de performanță

A se preciza indicatorii care permit monitorizarea progreselor și a realizărilor obținute.

Obiectiv: Crearea capacității de a pune în aplicare în mod eficace politicile UE în materie de securitate cibernetică și cooperarea operațională periodică/continuă care să permită o cooperare mai structurată între statele membre.

- Numărul de contribuții relevante din partea ENISA la punerea în aplicare a politicilor și inițiativelor legislative ale UE și naționale

- Feedback pozitiv din partea părților interesate cu privire la contribuțiile relevante ale ENISA

- Creștere cu 25 % față de nivelul de referință din 2023, astfel cum s-a raportat în raportul anual de activitate al ENISA (pentru numărul de contribuții relevante) și în conformitate cu sondajul anual al ENISA privind nivelul de satisfacție (pentru feedbackul pozitiv)

- Statistici privind utilizarea bazei de date a UE privind vulnerabilitatea

- Creștere cu 25 % a numărului de utilizatori comparativ cu 2025

Disponibilitatea, securitatea și funcționarea platformei CRA

- Reducerea cu 25 % a perioadelor de indisponibilitate a platformei și a numărului de incidente comparativ cu statisticile din 2025 privind perioadele de indisponibilitate și incidentele de pe platformă

Obiectiv: Dezvoltarea și implementarea unor mijloace și mecanisme pentru a sprijini și a aborda în mod eficace nevoile statelor membre, ale industriei și ale altor părți interesate.

- Numărul de părți interesate sprijinite de ENISA și calitatea sprijinului acordat.

- Numărul de măsuri implementate pentru a sprijini părțile interesate.

- Creșterea cu 10 % a numărului părților interesate care au beneficiat de sprijin și cu 10 % a nivelului de satisfacție al părților interesate care au beneficiat de sprijin comparativ cu 2025

Obiectiv: Crearea condițiilor prealabile pentru furnizarea mai rapidă a sistemelor de certificare a securității cibernetice determinate de nevoile pieței prin extinderea domeniului de aplicare al ECCF, prin asigurarea unei întrețineri eficace și a unor proceduri flexibile și prin creșterea transparenței.

- Numărul de sisteme adoptate

- Reducerea cu 50 % a timpului necesar pentru dezvoltarea unui sistem comparativ cu 2025

- Numărul de certificate valabile eliberate anual

- Creşterea cu 25 % faţă de scenariul de referinţă din 2025

- Feedback pozitiv din partea părţilor interesate cu privire la implicarea lor în dezvoltarea sistemelor şi transparenţa ECCF

- Creşterea cu 25 % faţă de nivelul de referinţă din sondajul anual privind nivelul de satisfacţie realizat de ENISA în comparaţie cu 2027

Obiectiv: Instituirea de mecanisme şi condiţii pentru a contribui la facilitarea respectării cerinţelor de securitate cibernetică, făcând astfel punerea lor în aplicare mai coerentă şi mai eficace.

- Procentul costurilor suportate de IMM-uri pentru respectarea NIS2 şi a normelor de securitate cibernetică, ca proporţie din toate costurile de asigurare a conformităţii

- >70 % IMM-uri care raportează o reducere a costurilor de asigurare a conformităţii pentru securitatea cibernetică comparativ cu 2025

- Numărul de atacuri de tip ransomware şi cuantumul daunelor în EUR

- Reducerea numărului de atacuri de tip ransomware cu >1 % faţă de 2027

- Procentul incidentelor transfrontaliere în timpul cărora sau după care autorităţile statelor membre au utilizat mecanisme de asistenţă reciprocă

- Creşterea proporţiei cazurilor în care s-a recurs la asistenţă reciprocă cu >20 de puncte procentuale comparativ cu 2025

Obiectiv: Reducerea dependenţelor critice prin dezvoltarea unui cadru coerent şi eficace la nivelul UE pentru a aborda riscurile la adresa securităţii lanţului de aprovizionare TIC.

- Numărul de măsuri adoptate

- Creşterea cu 25 % a numărului de măsuri adoptate şi a activelor esenţiale identificate în comparaţie cu data adoptării + 6 luni

- Reducerea dependenţelor de furnizorii cu grad ridicat de risc în ceea ce priveşte activele TIC esenţiale cu 25 % comparativ cu 2025

1.4. Obiectul propunerii/iniţiativei

☒ o acţiune nouă *(titlul IV Lanţul de aprovizionare, titlul V Simplificare)*

☐ o acţiune nouă întreprinsă ca urmare a unui proiect-pilot/a unei acţiuni pregătitoare[84]

☒ prelungirea unei acţiuni existente (*titlul II Mandatul ENISA şi titlul III Certificarea*)

☐ o fuziune sau o redirecţionare a uneia sau mai multor acţiuni către o altă/o nouă acţiune

[84] Astfel cum se menţionează la articolul 58 alineatul (2) litera (a) sau (b) din Regulamentul financiar.

1.5. Motivele propunerii/inițiativei

1.5.1. Cerința (cerințele) care trebuie îndeplinită (îndeplinite) pe termen scurt sau lung, inclusiv un calendar detaliat pentru punerea în aplicare a inițiativei

În iulie 2024, în orientările sale politice[85], președinta Comisiei Europene, Ursula von der Leyen, a solicitat simplificarea, consolidarea și codificarea legislației UE pentru a elimina orice suprapuneri și contradicții, menținând în același timp standarde ridicate. Scrisoarea de misiune adresată vicepreședintei executive Virkkunen[86] menționează, în special, îmbunătățirea procesului de adoptare a sistemelor europene de certificare a securității cibernetice și necesitatea de a ne proteja industriile, cetățenii și administrațiile publice împotriva amenințărilor interne și externe. În plus, în raportul Niinistö din 2024[87] se solicită reducerea riscurilor legate de dependențele nedorite de la nivelul lanțurilor de aprovizionare în ceea ce privește tehnologiile critice. Aspectele centrale ale rapoartelor Draghi[88] și Letta[89] comandate de președinta UE au reflectat asupra necesității ca piața unică să rămână competitivă prin simplificare și să asigure cele mai înalte niveluri de securitate și autonomie strategică. Pe această bază, revizuirea Regulamentului privind securitatea cibernetică este o piatră de temelie a activității Comisiei în materie de securitate și o introducere a unei revizuiri ambițioase a ecosistemului european de reglementare a securității cibernetice. Propunerea de Regulament privind securitatea cibernetică 2 introduce mecanisme de abordare a riscurilor în materie de securitate cibernetică la nivelul lanțurilor de aprovizionare și mecanisme de reducere a peisajului fragmentat al conformității și a complexității cadrelor orizontale și sectoriale. Se preconizează că ENISA va fi, de asemenea, un mijloc care va conduce la o mai mare simplificare a obligațiilor de raportare prin integrarea unui punct unic de intrare.

În plus, având în vedere numărul de dispoziții sectoriale introduse după 2019 pentru adoptarea Regulamentului privind securitatea cibernetică, precum și evoluția rapidă a peisajului amenințărilor la adresa securității cibernetice, mandatul ENISA trebuie revizuit pentru a stabili un set de sarcini mai bine orientate și reînnoite, cu scopul de a sprijini în mod eficace și eficient eforturile statelor membre, ale instituțiilor UE și ale altor părți interesate de a asigura un spațiu cibernetic securizat în Uniunea Europeană. Prin consolidarea Cadrului european de certificare a securității cibernetice (ECCF), propunerea asigură faptul că UE dispune de un sistem de certificare flexibil, modern și adaptabil, care va servi scopurilor acțiunilor din cadrul lanțului de aprovizionare și punerii în aplicare rapide a Regulamentului privind reziliența cibernetică. În concluzie, domeniul de aplicare propus al mandatului este delimitat, consolidând acele domenii în care agenția a demonstrat o valoare adăugată clară și adăugând acele noi domenii în care este nevoie de sprijin având în vedere noile priorități și instrumente de politică și pentru a consolida Fondul european de coeziune.

Prin urmare, revizuirea Regulamentului privind securitatea cibernetică este concepută ca o schimbare radicală majoră a posturii de securitate cibernetică a UE și a securității, pregătirii și rezilienței generale a Uniunii Europene.

85 Orientări politice 2024.
86 Scrisoarea de misiune a vicepreședintei executive Virkkunen.
87 Raportul elaborat de Sauli Niinistö.
88 Raportul Draghi privind competitivitatea UE.
89 Enrico Letta – *Much more than a market* (Mult mai mult decât o piață) (aprilie 2024).

1.5.2. Valoarea adăugată a intervenției UE (aceasta poate rezulta din diferiți factori, de exemplu mai buna coordonare, securitatea juridică, o mai mare eficacitate sau complementaritate). În sensul prezentei secțiuni, „valoarea adăugată a intervenției UE" este valoarea ce rezultă din acțiunea UE care depășește valoarea ce ar fi fost obținută dacă ar fi acționat doar statele membre.

Regulamentul privind securitatea cibernetică a fost adoptat în 2019 cu temeiul juridic al articolului 114 din TFUE, care împuternicește legiuitorul UE să adopte măsuri de armonizare a actelor cu putere de lege și a normelor administrative naționale care au ca obiectiv instituirea și funcționarea pieței interne.

Propunerea revizuită de regulament privind securitatea cibernetică vizează raționalizarea legislației în materie de securitate cibernetică la nivelul UE, completând și revizuind actualul Regulament privind securitatea cibernetică, în vigoare din 2019 (CSA1). Obiectivele din cadrul CSA1 de a acorda un mandat permanent Agenției Uniunii Europene pentru Securitate Cibernetică, dedicat sprijinirii nivelului comun ridicat de securitate cibernetică în întreaga UE, precum și cu scopul de a evita fragmentarea pieței interne în ceea ce privește sistemele de certificare a securității cibernetice, sunt menținute în cadrul revizuirii inițiate. Aceste obiective, astfel cum au fost deja analizate în mod corespunzător în propunerea de regulament privind securitatea cibernetică din 2017, nu pot fi realizate în mod satisfăcător de către statele membre, ci numai la nivelul Uniunii Europene, în conformitate cu articolul 5 din Tratatul privind Uniunea Europeană.

Propunerea de revizuire a Regulamentului privind securitatea cibernetică se axează în mod clar pe raționalizarea, definirea priorităților și codificarea sarcinilor în toate legislațiile legate de domeniul cibernetic numai la nivelul Uniunii Europene și în prezent nu există o astfel de inițiativă. Noua propunere consolidează și mai mult securitatea lanțului de aprovizionare și sectorul securității cibernetice în cadrul UE și sporește gradul de pregătire și reziliența statelor membre și a industriei. Dependențele de entități stabilite în țări terțe sau controlate de entități din țări terțe care prezintă motive de îngrijorare în materie de securitate cibernetică (furnizori cu grad ridicat de risc) afectează entități din întreaga Uniune, în timp ce incidentele de securitate cibernetică semnificative din lanțul de aprovizionare se răspândesc adesea dincolo de frontierele naționale. Este puțin probabil ca abordarea problemei doar la nivel național să fie eficientă.

Noile sarcini atribuite ENISA au o importanță crucială pentru atingerea unor niveluri ridicate de securitate cibernetică în întreaga UE. În pofida faptului că agenția lucrează în coordonare cu alte organisme de securitate ale UE, cum ar fi Europol, precum și cu Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică (ECCC), care este responsabil cu punerea în aplicare a finanțării, misiunea și sarcinile agenției sunt unice și, în prezent, nu există niciun alt organism care să aibă acest tip de responsabilități. În ecosistemul cibernetic al UE, toate entitățile implicate lucrează în sinergii strânse și în cadrul unor mandate clare. Prin urmare, propunerea CSA2 consolidează numai acele părți în care există o valoare adăugată clară, asigurându-se că nu există ambiguități în ceea ce privește duplicarea sarcinilor, pe fond, și nici în ceea ce privește finanțarea cu alte organisme din cadrul ecosistemului cibernetic.

În detaliu

Mandatul ENISA s-a extins prin acte legislative ulterioare, fără o revizuire cuprinzătoare a responsabilităților sale de bază și a resurselor de care dispune. Acest lucru a creat suprapuneri, ineficiențe și o prioritizare insuficientă a sarcinilor principale de sprijin pentru statele membre.

Mai multe state membre și-au pus în aplicare propriile sisteme naționale de certificare a securității cibernetice, care diferă în mod semnificativ în ceea ce privește domeniul de aplicare și procedurile de evaluare a conformității. Acest lucru creează fragmentare a pieței și sarcini redundante pentru operatori și IMM-uri, care doresc să fie certificați o singură dată și să își desfășoare activitatea în întreaga UE. ECCF a fost instituit în cadrul Regulamentului privind securitatea cibernetică pentru a aborda fragmentarea pieței, dar punerea în aplicare a fost lentă și inconsecventă.

În mod similar, mai multe acte juridice orizontale și sectoriale stabilesc măsuri de securitate cibernetică cu scopuri și obiective diferite, ceea ce duce, de asemenea, la diferențe în ceea ce privește abordările în materie de verificare a conformității și de supraveghere stabilite de statele membre. În consecință, entitățile, în special IMM-urile sau întreprinderile care își desfășoară activitatea în mai multe state membre, se confruntă cu o sarcină suplimentară de asigurare a conformității, ceea ce le afectează competitivitatea.

Abordările diverse în ceea ce privește securitatea lanțului de aprovizionare TIC și diferitele măsuri luate de statele membre conduc la fragmentarea pieței și la cerințe de conformitate diferite pentru entități. În special, având în vedere caracterul transfrontalier al lanțurilor de aprovizionare TIC, fragmentarea cerințelor de conformitate în cadrul pieței interne ar submina securitatea juridică pentru entități. Cadrele naționale diferite pentru restricționarea furnizorilor cu grad ridicat de risc riscă să creeze bariere în calea circulației transfrontaliere a bunurilor și serviciilor în cadrul pieței interne. În cele din urmă, întrucât lanțurile de aprovizionare TIC pot implica entități și infrastructuri critice, indiferent de locul în care sunt stabiliți furnizorii respectivi, fragmentarea și lacunele în ceea ce privește măsurile de securitate cibernetică creează riscuri de securitate suplimentare pentru entitățile respective.

În plus, propunerile de programe din cadrul financiar multianual (CFM) includ o dispoziție orizontală care impune excluderea furnizorilor cu grad ridicat de risc identificați în temeiul dreptului UE, pentru a proteja integritatea bugetului UE și pentru a se asigura că cheltuielile Uniunii nu contravin intereselor esențiale în materie de securitate ale Uniunii. Cadrul privind lanțul de aprovizionare din Regulamentul privind securitatea cibernetică ar fi mecanismul care permite această identificare în domeniul lanțurilor de aprovizionare TIC și, prin urmare, poate fi realizat numai la nivelul UE.

În mod implicit, atacurile cibernetice au un caracter transfrontalier, în special având în vedere efectele de propagare care ar putea apărea de la un singur punct de intrare afectat inițial. Amenințările și riscurile la adresa securității cibernetice au un impact asupra întregii Uniuni Europene și, prin urmare, un tablou colectiv al conștientizării situației ar putea îmbunătăți în mod semnificativ nivelurile de securitate cibernetică ale entităților din Uniunea Europeană. Propunerile din cadrul mandatului revizuit al ENISA abordează această chestiune cu obiectivul de a spori în mod semnificativ reziliența cibernetică a UE.

În concluzie, intervenția UE este esențială, deoarece amenințările la adresa securității cibernetice și provocările aferente se extind dincolo de statele membre individuale.

Soluțiile naționale fragmentate s-au dovedit insuficiente pentru a asigura încrederea și coordonarea la nivelul întregii piețe. Este necesar un cadru juridic revizuit al UE pentru a elimina barierele, a asigura punerea în aplicare coerentă și a sprijini statele membre într-un mediu de reglementare și de amenințări din ce în ce mai complex.

1.5.3. Învățăminte desprinse din experiențele anterioare similare

ENISA a fost înființată în 2004 cu un mandat fix. În 2019, a intrat în vigoare Regulamentul privind securitatea cibernetică, ale cărui dispoziții au acordat ENISA un mandat permanent și obiectivul de a deveni centrul de expertiză cibernetică în Europa. În prezent, ENISA este o marcă recunoscută și un partener de încredere în rândul părților interesate din UE. Competențele agenției au fost construite treptat în cursul a 25 de ani, reflectând evoluția ecosistemului cibernetic.

În conformitate cu articolul 67 din Regulamentul privind securitatea cibernetică, o dată la cinci ani, Comisia evaluează impactul, eficacitatea și eficiența ENISA și a practicilor sale de lucru, posibila necesitate a unor modificări și implicațiile financiare ale unor astfel de modificări. Evaluarea analizează, de asemenea, impactul, eficacitatea și eficiența dispozițiilor referitoare la cadrul european de certificare.

În conformitate cu dispozițiile, Comisia a efectuat o evaluare a agenției și a cadrului european de certificare a securității cibernetice, care a inclus o consultare publică și un studiu independent. În conformitate cu practicile privind o mai bună legiferare, Comisia a lansat, de asemenea, o consultare publică specifică privind revizuirea Regulamentului privind securitatea cibernetică, precum și o cerere de contribuții pentru a colecta date de la grupurile de părți interesate. Evaluarea a concluzionat că ENISA și-a îndeplinit mandatul obținând aproape toate realizările planificate. Obiectivele agenției rămân relevante în prezent, realizările sale fiind recunoscute în special de părțile interesate, cu precădere în perioade dificile, cum ar fi pandemia de COVID-19 și războiul de agresiune al Rusiei împotriva Ucrainei. În pofida feedbackului în general pozitiv din partea părților interesate cu privire la rezultatele ENISA, s-a arătat, de asemenea, că se mai pot aduce îmbunătățiri semnificative pentru a răspunde în mod consecvent așteptărilor părților interesate.

Învățămintele desprinse au demonstrat că, pentru a crește nivelul de eficiență, ENISA ar avea nevoie de mai multă orientare strategică, de definirea priorității sarcinilor și de 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 entitățile private, cu accent pe sprijinirea IMM-urilor. În cadrul tuturor consultărilor externe, s-a subliniat importanța creșterii finanțării, a personalului și a capacității operaționale a ENISA pentru a-i permite să răspundă cerințelor tot mai mari ale peisajului securității cibernetice din UE. În raportul său de evaluare, în urma studiului, serviciile Comisiei au evaluat necesitatea clară a unei legislații adaptate exigențelor viitorului, care să se poată adapta la peisajul complex și în evoluție rapidă al amenințărilor cibernetice și, respectiv, să consolideze agenția cu resursele necesare pentru a asigura sprijinul în vederea atingerii celor mai înalte niveluri de securitate cibernetică în Europa. Pe baza datelor colectate și a experienței dobândite în urma punerii în aplicare a Regulamentului privind securitatea cibernetică, s-a ajuns la concluzia că ar trebui raționalizată coordonarea cu alte organisme, precum și să se pună accentul pe sprijinul din partea ENISA pentru punerea în aplicare a dreptului UE și pe sprijinul

acordat Comisiei, la cerere, pentru elaborarea legislației legate de securitatea cibernetică. Propunerea analizează sinergiile cu prioritățile geopolitice ale Comisiei pentru a aborda riscuri precum dependențele tot mai mari de entități stabilite în țări care prezintă motive de îngrijorare în materie de securitate cibernetică (furnizori cu grad ridicat de risc) în Europa și controlate de acestea. În calitate de centru de expertiză, ENISA este în prezent și un registru esențial de informații care este esențial pentru construirea unei înțelegeri comune cu privire la amenințările și riscurile pe care le prezintă pentru entitățile UE. Prin urmare, cadrul propus se bazează pe experiența CSA1 și mobilizează coordonarea fluxurilor de informații în vederea compilării unui tablou holistic al conștientizării situației.

Evaluarea ECCF evidențiază mai multe recomandări strategice. 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 au evidențiat necesitatea unei revizuiri substanțiale a structurilor de guvernanță pentru a spori claritatea operațională și responsabilitatea la toate nivelurile, aspect abordat în propunerea de revizuire a Regulamentului privind securitatea cibernetică. Experiența funcționării actualului ECCF a demonstrat necesitatea de a moderniza și de a clarifica cadrul de certificare și de a introduce o procedură de întreținere pentru sistemele de certificare, pentru a le permite să se adapteze nevoilor pieței și situației amenințărilor. În cele din urmă, cadrul inițial nu a anticipat riscurile non-tehnice, care pot fi identificate ca o sursă de stagnare a punerii în aplicare a ECCF în ceea ce privește sistemele 5G și cloud.

Complexitatea ecosistemului cibernetic al UE a crescut în funcție de evoluția amenințărilor cibernetice. În observațiile scrise ale părților interesate, a existat un consens puternic cu privire la necesitatea de a reduce sarcina administrativă, în special pentru IMM-uri, și s-au solicitat proceduri simplificate de asigurare a conformității. Deși principalul efort de simplificare va fi canalizat prin intermediul inițiativei Omnibus digital, propunerea reflectă nevoile părților interesate prin introducerea unor modificări ale Directivei NIS 2 pentru a facilita procesul de punere în aplicare.

1.5.4. Compatibilitatea cu cadrul financiar multianual și posibilele sinergii cu alte instrumente corespunzătoare

CSA2 introduce revizuirile necesare pentru a dota UE cu instrumente și mecanisme care să răspundă peisajului și obiectivelor de politică în materie de securitate cibernetică. Regulamentul propus va consolida în continuare ENISA cu capacitățile necesare pentru a sprijini statele membre în punerea în aplicare a legislației UE și în combaterea riscurilor cibernetice. Având în vedere rapoartele Draghi și Letta menționate mai sus, propunerea privind cadrul financiar multianual (CFM) 2028-2034 plasează în centrul său competitivitatea, securitatea și autonomia strategică.

Prin urmare, propunerile din pachetul orizontal privind CFM 2028-2034, în special propunerile privind Fondul european pentru competitivitate și Orizont Europa, introduc noi criterii de eligibilitate bazate pe principiul excluderii „furnizorilor cu risc ridicat” de la primirea fondurilor UE. CSA2 este pe deplin aliniat la acest principiu și, în plus, reprezintă un instrument care permite punerea în aplicare a noilor cerințe privind „furnizorii cu risc ridicat”, deoarece oferă un cadru procedural pentru desemnarea țărilor care prezintă motive de îngrijorare în materie de securitate cibernetică la nivelul UE. În acest sens, CSA2 este o propunere strategică, în

conformitate cu prioritățile Comisiei pentru realizarea suveranității tehnologice și stimularea competitivității în Europa.

Eliminarea fragmentării existente va fi abordată printr-o mai mare armonizare a pieței de certificare a UE, ceea ce va face ca procesul european de certificare să fie mai eficient și mai durabil.

Propunerile privind CFM pentru perioada 2028-2034 consideră efortul de simplificare drept o prioritate în întregul cadru. Rubricile bugetare sunt comprimate la 4 în loc de 7, în timp ce numărul programelor de finanțare orizontale a fost redus semnificativ de la 52 la 16, oferind flexibilitate și adaptabilitate la nevoile actuale. Evaluarea impactului pentru revizuirea Regulamentului privind securitatea cibernetică a subliniat exact aceste obiective: necesitatea de a simplifica cerințele de securitate cibernetică în mai multe cadre legislative, de a codifica și de a concentra sarcinile ENISA asupra domeniilor cu cel mai mare impact pentru obținerea unei reziliențe sporite a ecosistemului cibernetic al UE. În urma acestor constatări, dispozițiile propuse stimulează competitivitatea prin simplificare; asigurarea unor niveluri ridicate de securitate printr-o mai bună coordonare și analiză a riscurilor și a vulnerabilităților; sprijinirea unor niveluri mai ridicate de armonizare prin depășirea fragmentării generate de numărul sistemelor naționale. În plus, ENISA este concepută ca vehicul principal care va stimula eforturile de simplificare digitală, deoarece va integra punctul unic de intrare pentru notificări, astfel cum se subliniază în inițiativa Omnibus digital[90].

O parte esențială a pachetului CFM 28-34 este propunerea privind un nou Fond pentru competitivitate (FEC), care reunește sub același acoperiș peste 16 programe de finanțare, cum ar fi programul Europa digitală, EU4Health, Fondul european de apărare etc. Orizont Europa va fi în continuare un program de sine stătător, strâns legat de FEC. Acest nou cadru de programare necesită o coordonare și o finanțare solide, care să corespundă priorităților actuale. În acest sens, dispozițiile propuse în CSA2 reprezintă baza pentru aprofundarea coordonării dintre ENISA și ECCC, responsabil de punerea în aplicare a programelor părților legate de securitatea cibernetică ale Europa digitală și Orizont Europa. Dispozițiile propuse asigură coerența și subliniază sinergiile dintre ENISA și ECCC. Aceeași abordare a fost adoptată în ceea ce privește cooperarea cu alte agenții și organisme, cum ar fi Europol.

Un alt aspect al alinierii dintre propunerea CSA2 și CFM 28-34 este principiul flexibilității. Odată cu revizuirea, Comisia propune un mecanism de „taxe”, care va oferi ENISA o modalitate flexibilă de a-și finanța parțial activitățile, mai precis cele legate de dezvoltarea și întreținerea sistemelor de atestare a competențelor în materie de securitate cibernetică, de prelucrarea și acordarea de autorizații furnizorilor și de întreținerea sistemelor europene de certificare a securității cibernetice. Prin această modificare, agenția va avea flexibilitatea și scalabilitatea necesare pentru a răspunde nevoilor părților interesate și va avea cheltuieli sustenabile prin refinanțarea serviciilor sale.

[90] A se adăuga după publicare.

1.5.5. Evaluarea diverselor opțiuni de finanțare disponibile, inclusiv a posibilităților de realocare a creditelor

De la ultima revizuire a mandatului ENISA în 2019, s-a înregistrat o tendință de creștere exponențială a contribuțiilor preconizate ale agenției la sprijinul pentru punerea în aplicare a legislației UE. Acest lucru a condus la solicitări de consolidare anuală a bugetului și a personalului peste nivelurile programate inițial. Revizuirea propusă introduce noi sarcini importante și include sarcinile mandatului ENISA, care au fost impuse prin alte acte legislative după adoptarea CSA1, extinzând astfel capacitățile ENISA, ceea ce necesită consolidări financiare și umane suplimentare. Determinată de obiectivul de a face din securitatea digitală avantajul competitiv al Europei, propunerea solicită un impact real în cadrul ecosistemului cibernetic. Acest lucru ar putea fi posibil numai cu investiții semnificative care să corespundă efectului dorit și, mai ales, nevoilor statelor membre și ale altor părți interesate. Noile sarcini includ nevoia de personal tehnic și specializat, precum și investiții financiare (de exemplu, pentru instrumente și platforme), care ar putea fi asigurate numai prin alocări financiare suplimentare de la bugetul UE.

Având ca obiectiv o mai mare flexibilitate și, în același timp, un buget sustenabil pe termen lung al agenției, revizuirea propune un mecanism de taxare care va finanța parțial serviciile furnizate pentru întreținerea cadrului de certificare a securității cibernetice și în ceea ce privește dezvoltarea și menținerea sistemelor de atestare europeană individuală a competențelor în materie de securitate cibernetică și prelucrarea și acordarea de autorizații furnizorilor.

Toate estimările privind resursele suplimentare în cadrul revizuirii Regulamentului privind securitatea cibernetică sunt efectuate din perspectiva bugetului de referință al ENISA din 2025 (costuri operaționale și ENI). Comisia a efectuat o analiză amplă a posibilităților de redistribuire în cadrul agenției pentru a ține seama de noile sarcini prevăzute în mandatul revizuit. Faptul că agenția lucrează la capacitățile sale maxime fără opțiuni de reducere a sarcinilor și cu o acțiune de reducere a unor priorități întreprinsă deja de consiliul de administrație în 2023 conduce în mod clar la concluzia că nicio sarcină nouă nu poate fi inclusă în structura actuală, fără a consolida atât bugetul, cât și resursele umane. În plus, multe dintre sarcinile actuale fac obiectul unor acorduri de contribuție între ENISA și Comisie. Prin urmare, propunerea urmărește să adauge aceste sarcini la mandatul ENISA și să primească un buget stabil pentru anii următori.

Fără a aduce atingere negocierilor privind următorul CFM, creditele alocate agenției începând cu 2028 vor fi compensate prin redistribuiri de la programele din CFM 2028-2034. În cazul în care este necesară o reducere compensatorie, resursele alocate agenției, precum și fluxurile și sursele de finanțare ale acestora ar putea necesita o revizuire. Măsurile instituite în cadrul CSA2 propus implică, de asemenea, preluarea unor sarcini suplimentare pentru direcția generală parteneră a ENISA (Direcția Generală Rețele de Comunicare, Conținut și Tehnologie, DG CNECT). Ar trebui remarcat în special faptul că cadrul lanțului de aprovizionare TIC va fi pus în aplicare pe deplin la nivelul Comisiei, inclusiv analiza de piață care însoțește evaluările riscurilor și elaborarea actelor de punere în aplicare. În plus, va fi necesar un set suplimentar de acte de punere în aplicare elaborate și adoptate de Comisie, în ceea ce privește modalitățile mecanismelor de taxare. Supravegherea și asistența suplimentare la nivelul Comisiei vor fi necesare pentru asigurarea respectării cadrului european de certificare a securității cibernetice, elaborarea de modele de

dispoziții, întreținerea sistemelor de securitate cibernetică, acordurile de recunoaștere reciprocă cu țările terțe și supravegherea ENISA.

1.6. Durata propunerii/inițiativei și a impactului său financiar

☐ **durată limitată**

– ☐ de la [ZZ/LL]AAAA până la [ZZ/LL]AAAA

– ☐ impactul financiar din AAAA până în AAAA pentru creditele de angajament și din AAAA până în AAAA pentru creditele de plată.

☒ **durată nelimitată**

– punere în aplicare cu o perioadă de creștere în intensitate din AAAA până în AAAA,

– urmată de o perioadă de funcționare la capacitate maximă.

1.7. Metoda (metodele) de execuție a bugetului planificată (planificate)

☐ **Gestiune directă** asigurată de Comisie

– ☐ prin intermediul serviciilor sale, inclusiv al personalului din delegațiile Uniunii

– ☐ prin intermediul agențiilor executive

☐ **Gestiune partajată** cu statele membre

☒ **Gestiune indirectă**, cu delegarea sarcinilor de execuție bugetară:

– ☐ țărilor terțe sau organismelor pe care le-au desemnat acestea

– ☐ organizațiilor internaționale și agențiilor acestora (a se preciza)

– ☐ Băncii Europene de Investiții și Fondului European de Investiții

– ☒ organismelor menționate la articolele 70 și 71 din Regulamentul financiar

– ☐ organismelor de drept public

– ☐ organismelor de drept privat cu misiune de serviciu public, cu condiția să li se furnizeze garanții financiare adecvate

– ☐ organismelor de drept privat dintr-un stat membru care sunt responsabile cu punerea în aplicare a unui parteneriat public-privat și cărora li se furnizează garanții financiare adecvate

– ☐ organismelor sau persoanelor cărora li se încredințează executarea unor acțiuni specifice în cadrul politicii externe și de securitate comună, în temeiul titlului V din Tratatul privind Uniunea Europeană, și care sunt identificate în actul de bază relevant

– ☐ organismelor stabilite într-un stat membru, reglementate de dreptul privat al unui stat membru sau de dreptul Uniunii și eligibile pentru a li se încredința, în conformitate cu normele sectoriale, execuția unor fonduri sau a unor garanții bugetare ale Uniunii, în măsura în care aceste organisme sunt controlate de organisme de drept public sau de organisme de drept privat cu misiune de serviciu public și beneficiază de garanții financiare adecvate care sunt furnizate sub formă de răspundere solidară din partea organismelor de control sau de garanții financiare echivalente și care pot fi limitate, pentru fiecare acțiune, la cuantumul maxim al sprijinului din partea Uniunii.

Observații

2. MĂSURI DE GESTIUNE

2.1. Dispoziții în materie de monitorizare și de raportare

Monitorizarea și raportarea vor respecta principiile enunțate în Regulamentul actual privind securitatea cibernetică[91], în Regulamentul financiar[92] și se vor efectua în conformitate cu Abordarea comună privind agențiile descentralizate[93].

În conformitate cu articolul 40 din Regulamentul financiar, ENISA trebuie să transmită anual Comisiei, Parlamentului European și Consiliului un document unic de programare (DUP) care să conțină programele de lucru anuale și multianuale și programarea resurselor. În plus, propunerea Comisiei de modificare a mandatului ENISA introduce cerința ca, în calitate de membru al consiliului de administrație, Comisia să exprime un vot pozitiv pentru adoptarea de către consiliul de administrație al ENISA a DUP, în ceea ce privește aspectele legate de resursele umane și de buget. De asemenea, Comisia va emite un aviz cu privire la proiectul de DUP înainte de desfășurarea procedurii de vot în cadrul consiliului de administrație, care ar trebui pusă în aplicare înainte de adoptarea DUP[94].

ENISA trebuie să prezinte consiliului de administrație un raport anual de activitate consolidat. Acest raport cuprinde, în special, informații privind realizarea obiectivelor și obținerea rezultatelor enunțate în documentul unic de programare. Raportul trebuie să fie transmis, de asemenea, Comisiei, Parlamentului European și Consiliului. Directorul executiv al ENISA ar trebui să prezinte o dată la doi ani consiliului de administrație o evaluare *ex post* a activităților ENISA. De asemenea, agenția ar trebui să elaboreze un plan de măsuri ulterioare în ceea ce privește concluziile evaluărilor retrospective și să prezinte Comisiei, de două ori pe an, un raport privind progresele înregistrate. Consiliului de administrație ar trebui să îi revină responsabilitatea monitorizării modului în care s-au luat măsuri adecvate în urma acestor concluzii.

Presupusele cazuri de administrare defectuoasă a activităților agenției fac obiectul investigațiilor efectuate de Ombudsmanul European în conformitate cu prevederile articolului 228 din tratat.

Sursele de date pentru monitorizarea planificată ar putea fi în cea mai mare parte ENISA, Grupul european pentru certificarea securității cibernetice, grupul de cooperare NIS, rețeaua CSIRT și autoritățile statelor membre. Pe lângă datele provenite din rapoartele (inclusiv rapoartele anuale de activitate) ENISA, ale Grupului european pentru certificarea securității cibernetice, ale Grupului de cooperare NIS și ale rețelei CSIRT și ale Comisiei, vor fi utilizate, atunci când este necesar, instrumente specifice de colectare a datelor (de exemplu, anchete adresate autorităților naționale, sondaje Eurobarometru, studii specifice și rapoarte din exercițiile paneuropene).

Propunerea Comisiei privind CSA2 continuă practica consacrată de revizuire și evaluarea agenției. Astfel cum se subliniază la articolul 119 din propunerea privind

91 Regulamentul UE privind securitatea cibernetică | EUR-Lex.

92 Regulamentul financiar aplicabil bugetului general al Uniunii (reformare) – Oficiul pentru Publicații al UE.

93 https://europa.eu/european-union/sites/europaeu/files/docs/body/joint_statement_and_common_approach_2012_en.pdf.

94 Regulamentul delegat - 2019/715 - RO - EUR-Lex.

CSA2, Comisia trebuie să comande o evaluare a ENISA până la [ZZ LL AAAA] și, ulterior, o dată la cinci ani. Această evaluare va analiza, în special, eventuala necesitate de a modifica mandatul ENISA și implicațiile financiare ale unei astfel de modificări. La fiecare a doua evaluare va exista o evaluare a rezultatelor obținute de ENISA având în vedere obiectivele, mandatul, misiunea, guvernanța și sarcinile sale, inclusiv o evaluare a măsurii în care continuarea activității ENISA este în continuare justificată în ceea ce privește obiectivele, mandatul, misiunea, guvernanța și sarcinile respective.

Evaluarea analizează, de asemenea, impactul, eficacitatea și eficiența dispozițiilor titlului III din regulament în ceea ce privește obiectivele cadrului european de certificare a securității cibernetice, asigurând un nivel adecvat de securitate cibernetică a produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate și a entităților din Uniune și îmbunătățind funcționarea pieței interne.

Evaluarea analizează, de asemenea, impactul, eficacitatea și eficiența dispozițiilor titlului IV din regulament în ceea ce privește obiectivele cadrului de securitate a lanțului de aprovizionare TIC.

Comisia raportează Parlamentului European, Consiliului cu privire la toate constatările și consiliului de administrație cu privire la constatările evaluării pentru titlul II din regulament. Rezultatele evaluării se fac publice.

2.2. Sistemul (sistemele) de gestiune și de control

2.2.1. Justificarea metodei (metodelor) de execuție bugetară, a mecanismului (mecanismelor) de punere în aplicare a finanțării, a modalităților de plată și a strategiei de control propuse

Având în vedere faptul că propunerea are un impact asupra contribuției anuale a UE la ENISA, bugetul UE va fi executat prin gestiune indirectă.

În temeiul principiului bunei gestiuni financiare, bugetul ENISA se execută pe baza principiului unui control intern eficace și eficient. Prin urmare, ENISA are obligația de a pune în aplicare o strategie de control corespunzătoare, coordonată între actorii competenți implicați în lanțul de control.

În ceea ce privește controalele *ex post*, ENISA, în calitate de agenție descentralizată, face în special obiectul:

- auditului intern efectuat de Serviciul de Audit Intern al Comisiei;
- rapoartelor anuale ale Curții de Conturi Europene, care furnizează o declarație de asigurare cu privire la fiabilitatea conturilor, precum și la legalitatea și regularitatea operațiunilor subiacente;
- descărcării anuale de gestiune acordate de Parlamentul European;
- unor posibile investigații efectuate de OLAF pentru a se asigura în special faptul că resursele alocate agențiilor sunt utilizate corespunzător.
- În calitate de direcție generală parteneră a ENISA, DG CNECT va pune în aplicare strategia sa de control privind agențiile descentralizate pentru a asigura furnizarea de date fiabile în cadrul raportului său anual de activitate. Cu toate că agențiile descentralizate au o responsabilitate deplină pentru

execuția bugetului lor, DG CNECT este responsabilă cu plata regulată a contribuțiilor anuale stabilite de autoritatea bugetară.

- În fine, Ombudsmanul European asigură un nivel suplimentar de control asupra ENISA și de răspundere în cadrul ENISA.

Pe baza evaluării efectuate de agenție și a evaluării impactului care a fost realizată pentru prezentarea propunerii de regulament privind securitatea cibernetică 2, s-a stabilit că este extrem de important să se asigure resurse financiare adecvate pentru ca ENISA să își îndeplinească sarcinile încredințate prin noul mandat. O noutate importantă pentru mandatul revizuit al agenției va fi introducerea unui mecanism de taxe care este avut în vedere pentru a finanța costurile de întreținere a sistemelor europene de certificare a securității cibernetice, adoptate în cadrul ECCF. ECCF revizuit va oficializa procedura de întreținere. Activitatea de întreținere va fi condusă de ENISA și va fi finanțată parțial din taxe pentru a ține seama de caracterul său scalabil (mai multe sisteme necesită mai mult personal pentru întreținere). Agenția va avea, de asemenea, capacitatea de a furniza instrumente de testare pentru a sprijini punerea în aplicare a procedurilor de evaluare a conformității atât în temeiul ECCF, cât și al altor acte legislative relevante ale UE în domeniul cibernetic. Modalitățile privind taxele vor fi stabilite într-un act de punere în aplicare, adoptat de Comisie. În plus, revizuirea are în vedere dezvoltarea și menținerea unor sisteme de atestare europeană individuală și emiterea de decizii privind autorizarea furnizorilor să elibereze atestate europene individuale de competențe în materie de securitate cibernetică.

2.2.2. Informații privind riscurile identificate și sistemul (sistemele) de control intern instituit(e) pentru atenuarea lor

Propunerea de regulament privind securitatea cibernetică 2 ca atare vizează atenuarea riscurilor identificate în cadrul mandatului ENISA și al cadrului ECCF, inclusiv cadrul de securitate a lanțului de aprovizionare TIC și dispozițiile de simplificare. Mai precis, ENISA este o agenție a Uniunii Europene care există deja și, în cadrul revizuirii, mandatul este delimitat în continuare, consolidând domeniile în care agenția a demonstrat o valoare adăugată clară și adăugând acele noi domenii în care este nevoie de sprijin având în vedere noile priorități și instrumente de politică, cum ar fi simplificarea prin integrarea unui punct unic de intrare pentru raportare; sprijinirea unui tablou comun al conștientizării situației la nivel european și a cooperării operaționale, consolidarea și raționalizarea cadrului european de certificare a securității cibernetice.

Un alt risc identificat și abordat în propunere este numărul de acorduri de contribuție pe care Comisia și agenția le-au încheiat în ultimii ani. Având în vedere situația geopolitică actuală și evoluția rapidă a peisajului amenințărilor la adresa securității cibernetice, Comisia a încheiat acorduri de contribuție cu agenția în valoare totală de peste 75 de milioane EUR începând din 2019. Având în vedere că sarcinile încredințate ENISA prin acordurile respective au în prezent un caracter permanent, fluxul instabil al bugetului prin intermediul acordurilor de contribuție prezintă un risc pentru obținerea pe termen lung a rezultatelor activităților ENISA.

Prin urmare, prezenta propunere se referă, printre altele, la consolidarea capacității agenției în materie de resurse, la redefinirea sarcinilor sale și la creșterea eficienței. În special, posibilitatea de a colecta taxe va sprijini pe termen lung un circuit financiar sustenabil al agenției prin refinanțarea costurilor legate de întreținerea sistemelor europene de certificare, adoptate în cadrul ECCF, de testarea

instrumentelor și de dezvoltarea, întreținerea și punerea în aplicare a sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică. Pe termen lung, se estimează că se vor realiza economii la bugetul UE, ajungând la 18,5 milioane EUR pe an. Comisia va fi lider în ceea ce privește modalitățile de percepere a taxelor și componența acestora prin adoptarea de acte de punere în aplicare.

Creșterea sarcinilor operaționale ale agenției nu reprezintă un risc real. Aceste sarcini ar completa acțiunea statelor membre și le-ar sprijini, la cerere. Acestea se vor limita, de asemenea, la servicii predefinite, prin analogie cu Regulamentul (UE) 2019/881 privind securitatea cibernetică[95]. Noile elemente/sarcini din propunere vor aduce valoare adăugată pentru părțile interesate europene care ar beneficia de pe urma faptului că ENISA este un centru de informații, contribuind la schimbul de informații și furnizând notificări de alertă entităților lor constitutive.

În plus, modelul propus al agenției este aliniat la abordarea comună a Comisiei în ceea ce privește agențiile descentralizate, asigurându-se că există un control suficient pentru a prevedea că ENISA acționează în vederea atingerii obiectivelor sale. Riscurile operaționale și financiare ale modificărilor propuse par a fi limitate, deoarece dispozițiile sunt compuse pentru a atenua riscurile actuale. Cu toate acestea, anumite aspecte negative ar putea fi preconizate pe termen lung, în ceea ce privește:

- resurse operaționale limitate din cauza nevoilor operaționale tot mai mari ale statelor membre și a riscurilor și amenințărilor cibernetice în continuă evoluție în domeniul securității cibernetice;

- un buget majorat rapid, cu așteptări privind o punere în aplicare rapidă;

- lipsa unor niveluri adecvate de resurse financiare și umane care să corespundă nevoilor operaționale.

2.2.3. Estimarea și justificarea raportului cost-eficacitate al controalelor (raportul dintre costurile controalelor și valoarea fondurilor aferente gestionate) și evaluarea nivelurilor estimate ale riscurilor de eroare (la plată și la închidere)

Costurile suportate de DG CNECT pentru monitorizarea și supravegherea entităților cărora le-a fost încredințată execuția, inclusiv ENISA, sunt de aproximativ 5,25 milioane EUR, astfel cum s-a raportat în raportul anual de activitate pentru 2024[96]. Această sumă include în principal costurile cu personalul și reprezintă 0,50 % din plățile operaționale efectuate către aceste entități în cursul anului 2024. Rata globală a costului controalelor a crescut ușor la 0,50 % în 2024, de la 0,46 % în 2023, dar rămâne relativ stabilă în comparație cu anii precedenți.

Mai precis, în ceea ce privește ENISA, costurile de control în 2024 se ridică la 0,32 milioane EUR sau 0,70 % din costurile de control în 2024, comparativ cu 0,69 % în 2023 și 1,22 % în 2022. Potrivit analizei, costurile mai ridicate ale controlului sunt asociate în principal pregătirii și monitorizării acordurilor de contribuție dintre Comisie și agenție (în principal costul resurselor umane), care se preconizează că vor fi reduse în mod semnificativ în noul mandat și, prin urmare, se preconizează niveluri mai ridicate de eficiență. În ceea ce privește costurile totale pentru DG CNECT în

95 https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.

96 CNECT_AAR_2024_final.

comparație cu celelalte entități cărora le-a fost încredințată execuția, ENISA se află la mijloc, în comparație cu alte 11 entități.

Propunerea privind CSA2 prevede o creștere a personalului DG CNECT cu 50 ENI, din care 1 ENI suplimentar va fi alocat în mod specific pentru sarcinile legate de faptul că DG CNECT este DG parteneră a agenției. Această persoană va sprijini pregătirea avizului Comisiei privind documentul unic de programare al ENISA și va monitoriza punerea în aplicare a acestuia; va sprijini supravegherea întocmirii bugetului agenției și va monitoriza execuția acestuia. Va acorda asistență agenției în ceea ce privește dezvoltarea activităților sale în concordanță cu politicile Uniunii, inclusiv prin participarea la reuniuni relevante. Acțiunea este justificată de sarcinile sporite de monitorizare pentru DG CNECT, care, printre altele, intenționează să exprime un vot pozitiv al Comisiei cu privire la aspecte legate de buget și de resursele umane. Ar trebui remarcat faptul că procesul de punere în aplicare a dispozițiilor referitoare la desemnarea țărilor care prezintă riscuri strategice în materie de securitate cibernetică pentru anumiți furnizori de active esențiale cu grad ridicat de risc va fi condus pe deplin de Comisie. Necesarul estimat de personal pentru evaluările riscurilor în legătură cu cele de mai sus este de 25 ENI. Acțiunea este justificată de volumul de muncă necesar pentru punerea în aplicare a cadrului de politică, mai precis sprijinul pentru coordonarea de către UE a evaluărilor riscurilor; analiza economică pentru fiecare produs/serviciu TIC; elaborarea actelor de punere în aplicare respective și monitorizarea punerii în aplicare a cadrului; efectuarea de evaluări privind proprietatea și controlul. Potrivit estimărilor, costurile controalelor suportate de Comisie pentru punerea în aplicare a cadrului privind lanțul de aprovizionare vor fi afectate în mod specific de numărul de evaluări pe care le va efectua Comisia referitoare la structura de proprietate și la mecanismele de control. Cu toate acestea, rezultatele acestei sarcini vor contribui în mare măsură la realizarea de economii pentru statele membre în cadrul supravegherii punerii în aplicare a măsurilor de atenuare și a obligațiilor impuse entităților NIS 2 prin acest cadru. Statele membre vor fi în măsură să valorifice rezultatele evaluărilor referitoare la structura de proprietate și la mecanismele de control în mod direct, față de situația în care fiecare în parte ar cheltui resurse pentru aceleași nevoi de evaluare. Consolidarea cadrului european de certificare a securității cibernetice, standardizarea și punerea în aplicare a activităților conexe, punerea în aplicare a Directivei NIS 2 (inclusiv nevoile de punere în aplicare respective, actele de punere în aplicare privind taxele și sprijinirea întreținerii sistemelor de certificare și a sistemelor de atestare a competențelor) au fost estimate la 19 ENI, în timp ce politicile de cooperare operațională și de conștientizare a situației necesită încă 5 ENI. Descriere completă a sarcinilor în secțiunea 3.2.4.

În raportul său anual de activitate consolidat pe 2023[97], ENISA a formulat o concluzie pozitivă cu privire la evaluarea sistemelor sale de control intern și a furnizat o declarație de asigurare fără rezerve. În raportul său anual privind agențiile UE pentru exercițiul financiar 2023, CCE a emis o opinie de audit fără rezerve cu privire la conturi și o opinie cu rezerve privind legalitatea și regularitatea plăților subiacente conturilor (menționată și în 2.2.2). DG CNECT a luat act de raport, însă a concluzionat că acesta nu are un impact asupra eficacității supravegherii CNECT. De asemenea, ENISA raportează periodic cu privire la măsurile luate pentru a preveni repetarea constatărilor și, până în prezent, nu există indicii că rata de eroare se va înrăutăți/va depăși 2 % în anii următori.

[97] enisa.europa.eu/sites/default/files/2024-11/2023 Consolidated Annual Activity Report_1.pdf.

În plus, articolul 80 alineatul (2) din Regulamentul financiar al ENISA[98] prevede posibilitatea ca agenția să partajeze o structură de audit intern cu alte organisme ale Uniunii care își desfășoară activitatea în același domeniu de politică, în cazul în care capacitatea de audit intern a unui singur organism al Uniunii nu este eficientă din punctul de vedere al costurilor.

În concluzie, având în vedere creșterea propusă a dimensiunii agenției cu peste 100 %, comparativ cu creșterea relativ scăzută a costurilor de control, analiza arată un raport satisfăcător cost-eficacitate. Având în vedere toate datele disponibile, nu există niciun indiciu că rata de eroare preconizată ar putea fi mai mare de 2 %.

2.3. Măsuri de prevenire a fraudelor și a neregulilor

Agenția Uniunii Europene pentru Securitate Cibernetică va aplica cele mai înalte standarde aplicabile pentru prevenirea fraudei și a neregulilor.

Personalul agenției verifică plățile pentru orice fel de servicii sau de studii solicitate, înainte de efectuarea plății, luând în considerare toate obligațiile contractuale, principiile economice și bunele practici financiare sau de gestionare. Toate acordurile și contractele încheiate între agenție și beneficiarii plăților vor cuprinde dispoziții antifraudă (control, cerințe privind raportarea etc.);

Pentru a combate frauda, corupția și alte activități ilicite, se aplică fără restricție dispozițiile Regulamentului (UE, Euratom) nr. 883/2013 al Parlamentului European și al Consiliului.

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

3.1. Rubrica (rubricile) din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate)

- Linii bugetare existente

În ordinea rubricilor din cadrul financiar multianual și a liniilor bugetare.

Rubrica din cadrul financiar multianual	Linia bugetară	Tipul de cheltuieli	Contribuție			
	Numărul	Dif./Nedif.[99]	din partea țărilor AELS[100]	din partea țărilor candidate și potențial candidate[101]	din partea altor țări terțe	alte venituri alocate
	[XX.YY.YY.YY]	Nedif.	DA	NU	NU	DA/NU
	[XX.YY.YY.YY]	Dif./Nedif.	DA/NU	DA/NU	DA/NU	DA/NU

98 MB Decision 2019_8 Financial rules_adopted.pdf.
99 Dif. = credite diferențiate / Nedif. = credite nediferențiate.
100 AELS: Asociația Europeană a Liberului Schimb.
101 Țările candidate și, după caz, candidații potențiali din Balcanii de Vest.

	[XX.YY.YY.YY]	Dif./Nedif.	DA/NU	DA/NU	DA/NU	DA/NU

- Noile linii bugetare solicitate

<u>În ordinea</u> rubricilor din cadrul financiar multianual şi a liniilor bugetare.

Rubrica din cadrul financiar multianual	Linia bugetară	Tipul de cheltuieli	Contribuție			
	Numărul	Dif./Nedif.	din partea țărilor AELS	din partea țărilor candidate și potențial candidate	din partea altor țări terțe	alte venituri alocate
	[XX.YY.YY.YY]	Dif./Nedif.	DA/NU	DA/NU	DA/NU	DA/NU
	[XX.YY.YY.YY]	Dif./Nedif.	DA/NU	DA/NU	DA/NU	DA/NU
	[XX.YY.YY.YY]	Dif./Nedif.	DA/NU	DA/NU	DA/NU	DA/NU

3.2. Impactul financiar estimat al propunerii asupra creditelor

3.2.1. Sinteza impactului estimat asupra creditelor operaționale

– ☐ Propunerea/inițiativa nu implică utilizarea de credite operaționale

– ☒ Propunerea/inițiativa implică utilizarea de credite operaționale, conform explicațiilor de mai jos

3.2.1.1. Credite din bugetul votat

milioane EUR (cu trei zecimale)

Agenția: ENISA	Anul **2028**	Anul **2029**	Anul **2030**	Anul **2031**	Anul **2032**	Anul **2033**	Anul **2034**	**TOTAL CFM 2028-2034**
Linia bugetară: <…….> / Contribuția de la bugetul UE pentru agenție	20,900 €	20,594 €	25,338 €	26,801 €	26,801 €	26,301 €	26,301 €	173,006

Creditele/contribuția de la bugetul UE pentru agenție vor fi compensate/va fi compensată printr-o reducere a pachetului financiar al următorului program <…….>/linie bugetară: <…….> /în anul (anii): <…….> .

			Anul **2028**	Anul **2029**	Anul **2030**	Anul **2031**	Anul **2032**	Anul **2033**	Anul **2034**	**TOTAL CFM 2028-2034**	
TOTAL credite operaționale	Angajamente	(4)	20,900 €	20,594 €	25,338 €	26,801 €	26,801 €	26,301 €	26,301 €	173,006	
	Plăți	(5)	20,900 €	20,594 €	25,338 €	26,801 €	26,801 €	26,301 €	26,301 €	173,006	
TOTAL credite cu caracter administrativ finanțate din bugetul unor programe specifice		(6)	1,365	`1,365	1,470	1,785	2,100	2,415	2,625	**13,125**	
TOTAL credite în cadrul RUBRICII 2	Angajamente		=4+6	22,265 €	21,959 €	26,808 €	28,586 €	28,901 €	28,716 €	28,926 €	186,161

din cadrul financiar multianual	Plăți	=5+6	22,265 €	20,890 €	24,851 €	26,254 €	26,254 €	25,754 €	25,754 €	186,161

DG: CNECT	Anul **2028**	Anul **2029**	Anul **2030**	Anul **2031**	Anul **2032**	Anul **2033**	Anul **2034**	**TOTAL CFM 2028-2034**
• Resurse umane	**3,693**	**3,693**	**4,574**	**5,277**	**5,980**	**6,683**	**7,475**	**37,375**
• Alte cheltuieli administrative	0	0	0	0	0	0	0	**0**

TOTAL PENTRU DG CNECT	Credite	**3,693**	**3,693**	**4,574**	**5,277**	**5,980**	**6,683**	**7,475**		**37,375**

TOTAL credite în cadrul RUBRICII 4 din cadrul financiar multianual	(Total angajamente = Total plăți)	**2,328**	**2,328**	**3,104**	**3,492**	**3,880**	**4,268**	**4,850**	**24,25**

milioane EUR (cu trei zecimale)

		Anul **2028**	Anul **2029**	Anul **2030**	Anul **2031**	Anul **2032**	Anul **2033**	Anul **2034**	**TOTAL CFM 2028-2034**
TOTAL credite în	Angajamente	24,594	24,257	29,912	32,078	32,781	32,984	33,776	210,38

cadrul RUBRICILOR 1-4										
din cadrul financiar multianual	Plăți	24,594	24,257	29,912	32,078	32,781	32,984	33,776	210,38	

3.2.2. Realizările preconizate finanțate din credite operaționale (nu se completează pentru agențiile descentralizate)

Credite de angajament în milioane EUR (cu trei zecimale)

A se indica obiectivele și realizările ⇩			Anul **2028**		Anul **2029**		Anul **2030**		Anul **2031**		A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea secțiunea 1.6)						**TOTAL**	
	REALIZĂRI																	
	Tip[102]	Costuri medii	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Total nr.	Total costuri
OBIECTIVUL SPECIFIC nr. 1[103] …																		
– Realizare																		
– Realizare																		
– Realizare																		
Subtotal pentru obiectivul specific nr. 1																		
OBIECTIVUL SPECIFIC nr. 2 …																		

102 Realizările se referă la produsele și serviciile care trebuie furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de drumuri construiți etc.).

103 Conform descrierii din secțiunea 1.3.2. „Obiectiv(e) specific(e)”.

– Realizare																		
Subtotal pentru obiectivul specific nr. 2																		
TOTALURI																		

3.2.3. Sinteza impactului estimat asupra creditelor administrative

– ☐ Propunerea/inițiativa nu implică utilizarea de credite cu caracter administrativ

– ☒ Propunerea/inițiativa implică utilizarea de credite cu caracter administrativ, conform explicațiilor de mai jos

3.2.3.1. Credite din bugetul votat

(suplimentar)

CREDITE VOTATE	Anul **2028**	Anul **2029**	Anul **2030**	Anul **2031**	Anul **2032**	Anul **2033**	Anul **2034**	**TOTAL 2028-2034**
RUBRICA 4								
Resurse umane	2,328	2,328	3,104	3,492	3,880	4,268	4,840	24,25
Alte cheltuieli administrative	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Subtotal de la RUBRICA 4	2,328	2,328	3,104	3,492	3,880	4,268	4,840	24,25
În afara RUBRICII 4								
Resurse umane	1,365	1,365	1,470	1,785	2,100	2,415	2,625	**13,125**
Alte cheltuieli cu caracter administrativ	0,000	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**
Subtotal în afara RUBRICII 4	**1,365**	**1,365**	**1,470**	**1,785**	**2,100**	**2,415**	**2,625**	**13,125**
TOTAL	**3,693**	**3,693**	**4,574**	**5,277**	**5,980**	**6,683**	**7,475**	**37,375**

3.2.4. Necesarul de resurse umane estimat (suplimentar)

– ☐ Propunerea/inițiativa nu implică utilizarea de resurse umane

– ☒ Propunerea/inițiativa implică utilizarea de resurse umane, conform explicațiilor de mai jos

3.2.4.1. Finanțare din bugetul votat

Estimări în echivalent normă întreagă (ENI)[104]

CREDITE VOTATE	Anul **2028**	Anul **2029**	Anul **2030**	Anul **2031**	Anul **2032**	Anul **2033**	Anul **2034**
•Posturi din schema de personal (funcționari și agenți temporari)							
20 01 02 01 (la sediu și în reprezentanțele Comisiei)	12	12	16	18	20	22	25
20 01 02 03 (delegațiile UE)	0	0	0	0	0	0	0
(cercetare indirectă)	0	0	0	0	0	0	0
(cercetare directă)	0	0	0	0	0	0	0
Alte linii bugetare (a se preciza)	0	0	0	0	0	0	0
• Personal extern (în ENI)							

104 Vă rugăm să precizați după tabel câte ENI din numărul indicat sunt deja alocate gestionării acțiunii și/sau pot fi redistribuite în cadrul DG-ului pe care îl reprezentați și care este valoarea nevoilor dumneavoastră nete.

20 02 01 (AC, END din „pachetul global”)		0	0	0	0	0	0	0
20 02 03 (AC, AL, END și JPD în delegațiile UE)		0	0	0	0	0	0	0
Linia de sprijin administrativ	- la sediu	0	0	0	0	0	0	0
[XX.01.YY.YY]	- în delegațiile UE	0	0	0	0	0	0	0
(AC, END – cercetare indirectă)		0	0	0	0	0	0	0
(AC, END – cercetare directă)		0	0	0	0	0	0	0
Alte linii bugetare (a se preciza) – rubrica 4		0	0	0	0	0	0	0
Alte linii bugetare (a se preciza) – în afara rubricii 4		13	13	14	17	20	23	25
TOTAL		**25**	**25**	**30**	**35**	**40**	**45**	**50**

Personalul necesar pentru punerea în aplicare a propunerii (în ENI):

	Personal ce urmează să fie acoperit de personalul actual disponibil în cadrul serviciilor Comisiei	**În mod excepțional, personal suplimentar**		
		Personal ce urmează să fie finanțat în cadrul rubricii 7 sau Cercetare	**Personal ce urmează să fie finanțat de la linia BA**	**Personal ce urmează să fie finanțat din taxe**
Posturi din schema de personal		25		
Personal extern (AC, END, INT)			25	

Impactul estimat asupra cheltuielilor și a personalului pentru 2028 și ulterior este orientativ și nu aduce atingere următorului cadru financiar multianual. Sursa de finanțare și domeniul de aplicare al angajamentului financiar al Uniunii pentru perioada de după 2027 depind în continuare de rezultatul negocierilor interinstituționale privind CFM 2028-2034, de procedura bugetară anuală și de mecanismul de coordonare.

Descrierea sarcinilor care trebuie îndeplinite de direcția generală sectorială din cadrul Comisiei

Funcționari și personal temporar	**Coordonarea ENISA (1)**: Reprezentarea Comisiei în cadrul consiliului de administrație al agenției; Elaborarea avizului Comisiei privind documentul unic de programare al ENISA și monitorizarea punerii în aplicare a acestuia. Supravegherea întocmirii bugetului agenției și monitorizarea execuției sale. Acordarea de asistență agenției în ceea ce privește dezvoltarea activităților sale în concordanță cu politicile Uniunii, inclusiv prin participarea la reuniuni relevante. **Sisteme de atestare a competențelor/Academia de competențe (2)**: Va fi nevoie de personal suplimentar în cadrul CNECT pentru a elabora acte de punere în aplicare de stabilire a taxelor pe care ENISA le va percepe solicitanților pentru a deveni furnizori autorizați. Aceste acte de punere în aplicare vor fi cel puțin 12, câte unul pentru fiecare profil ECSF. **Lanțul de aprovizionare** (25) Sprijinirea pregătirii evaluărilor coordonate ale riscurilor la nivelul Uniunii. Efectuarea de analize economice pentru fiecare dintre produsele și serviciile TIC avute în vedere. Elaborarea actelor de punere în aplicare respective privind identificarea activelor esențiale, măsurile de atenuare propuse și desemnarea țărilor care prezintă riscuri strategice în materie de securitate cibernetică pentru anumite active esențiale, identificarea furnizorilor cu grad ridicat de risc, verificarea cererilor de derogare și pregătirea deciziilor Comisiei. Sprijinirea punerii în aplicare și a supravegherii măsurilor adoptate. **Cadrul european de certificare a securității cibernetice, standardizarea și punerea în aplicare a activităților conexe, punerea în aplicare a Directivei NIS 2 (17)**: Asigurarea respectării Regulamentului privind securitatea cibernetică, în special guvernanța organismelor de evaluare a conformității (contestarea competenței organismelor de evaluare a conformității) Implicarea părților interesate (și Adunarea) Recunoaștere reciprocă cu țările terțe Elaborarea unui act de punere în aplicare standardizat (cereri detaliate care fac obiectul consultărilor și elaborarea unor modele de dispoziții) Menținerea sistemului, revizuire juridică, procedura de comitologie Coordonarea cu GC NIS și întreținerea sistemului pentru entități Acte de punere în aplicare în temeiul Directivei NIS 2 Alinierea organismelor de evaluare a conformității la Regulamentul privind securitatea cibernetică, prezumția de conformitate + standardizarea Coordonarea dintre supravegherea pieței și ANCC Alinierea tehnică dintre Regulamentul privind reziliența cibernetică și sistemele de certificare **Coordonarea operațională și conștientizarea situației (5)**: Expertiză sectorială și în materie de actori care generează amenințări pentru a contribui la conștientizarea situației amenințărilor la adresa infrastructurii critice la nivelul UE, inclusiv prin intermediul tehnologiilor emergente Coordonarea cu ENISA și cu alte entități și rețele ale UE în vederea pregătirii pentru incidentele cibernetice semnificative și de mare amploare

Personal extern	La fel ca mai sus

Descrierea sarcinilor suplimentare care urmează să fie îndeplinite de ENISA:

Funcționari și personal temporar	Gestionarea rezervei UE pentru securitate cibernetică (manageri de țară și sprijin pentru punerea în aplicare, în timp ce costurile operaționale reale ale rezervei sunt acoperite astfel cum se prevede în Regulamentul privind solidaritatea cibernetică) (10) Gestionarea în temeiul Regulamentului privind reziliența cibernetică a Platformei unice de raportare (SRP) (exploatare) (9) Servicii de vulnerabilitate legate de SRP (4) Extinderea SRP la punctul unic de intrare (dezvoltare & exploatare) (8) Elaborarea de orientări tehnice, expertiză în materie de securitate a produselor și analize de piață pentru a sprijini punerea în aplicare a Regulamentului privind reziliența cibernetică (7) Standardizarea în sprijinul punerii în aplicare a Regulamentului privind reziliența cibernetică/a certificării/a NIS2 (4) Sprijinirea activităților de supraveghere a pieței în temeiul Regulamentului privind reziliența cibernetică (4) Sprijinirea testării conformității și a evaluărilor de securitate ale produselor (4) Sprijinirea statelor membre în ceea ce privește asistența reciprocă (3) Furnizarea de servicii de gestionare a vulnerabilităților, menținerea EUVD și furnizarea de funcții de consiliere și de îmbogățire (CVD) (15) Cooperare operațională & conștientizarea situației – platforme de atenuare și de sprijin, cum ar fi CNW/CyCLONe; sprijinirea sarcinilor legate de notificările de alertă; sprijinirea coordonării consolidate cu alte entități relevante pentru a dezvolta registre de informații verificate și fiabile privind amenințările cibernetice [articolul 11 alineatul (1a) din CSA2] (5) Sprijin pentru reziliența sectoarelor critice (inclusiv punerea în aplicare a Planului de acțiune privind securitatea cibernetică în domeniul sănătății) (4) Dezvoltarea sistemului de atestare a competențelor (2) Întreținerea și supravegherea sistemului de atestare a competențelor (6) Administrative (contabil pentru taxe/HR/IT) (8) Întreținerea sistemelor de certificare (11) Sarcini orizontale – implicarea sporită a părților interesate, elaborarea specificațiilor tehnice și implicarea în activități de standardizare în sprijinul sistemelor (1)
Personal extern	La fel ca mai sus Două END obligatorii pentru fiecare stat membru pentru a sprijini activitățile agenției și pentru a servi drept ofițeri naționali de legătură, cu accent pe cooperarea operațională și pe divulgarea coordonată a vulnerabilităților. (13) Se consideră că ceilalți 27 END nu implică costuri și, prin urmare, nu au implicații bugetare.

Costuri operaționale suplimentare pe an pentru ENISA 2028-2034:

Costuri	Buget	Calendar	Explicație
Site-ul privind competențele în materie de securitate cibernetică	750 000 EUR	50 % în 2029 50 % în 2030	Pentru a asigura transparența procedurilor, propunerea impune ENISA să mențină un site web cu profiluri ECFS, sisteme de atestare, informații privind taxele pentru fiecare sistem, taxele recomandate pentru fiecare atestare și lista furnizorilor de atestate autorizați.
Divulgarea coordonată a vulnerabilităților (CVD)	1 milion EUR	Începând cu 2028	Securitatea produselor și a serviciilor utilizate în infrastructura noastră critică depinde foarte mult de schimbul de informații în timp util cu privire la vulnerabilitățile descoperite și la modul în care acestea pot fi atenuate.
Informații privind amenințările la adresa securității cibernetice	3 milioane EUR	Începând cu 2028	Pentru crearea unui tablou al conștientizării situației realizat în cooperare, ENISA și Comisia.

Punct unic de intrare	8 milioane EUR	6 milioane EUR în 2028 500 000 EUR în 2029 500 000 EUR în 2030 500 000 EUR în 2031 500 000 EUR în 2032	Pentru a putea îndeplini propunerea Omnibus digital a Comisiei de simplificare a respectării obligațiilor de raportare a incidentelor de securitate cibernetică și a încălcării securității datelor prin dezvoltarea și menținerea unui punct unic de intrare.
Întreținerea SRP în temeiul Regulamentului privind reziliența cibernetică și altele	3 milioane EUR	Începând cu 2028	SRP introdus de colegiuitori este cel mai mare sistem informatic dezvoltat vreodată în istoria ENISA și un pilon esențial al Regulamentului privind reziliența cibernetică. În prezent, unitatea este finanțată printr-un acord de contribuție, dar gestionarea sa curentă va necesita ENI (a se vedea mai sus), precum și costuri operaționale. ENISA joacă un rol esențial în asigurarea

			succesului cadrului Uniunii privind securitatea produselor, Regulamentul privind reziliența cibernetică.
Comunicarea securizată și maturitatea în materie de securitate cibernetică a ENISA	Peste 2 milioane EUR.	Investiții în valoare de 1,1 milioane EUR în 2028 (platformele CyCLONe/CSIRT + sec comms) 1 milion EUR pe an întreținere începând din 2029 1,5 milioane EUR maturitatea cibernetică	Asigurarea securității cibernetice a agenției și a instrumentelor de comunicare.
Întreținerea certificării de securitate cibernetică	1 400 000 de milioane EUR	600 000 în 2028 1 000 000 în 2029 1 200 000 în 2030 1 400 000 în 2031 1 400 000 în 2032 1 400 000 în 2033 1 400 000 în 2034	Acoperite de taxe (integral începând cu 2032)
Sisteme de atestare a securității cibernetice	212 920 EUR	Începând din 2030, 50 % erau acoperite de bugetul UE	Acoperite integral de taxe începând cu 2033

3.2.5. Prezentare generală a impactului estimat asupra investițiilor legate de tehnologia digitală

Obligatoriu: în tabelul de mai jos trebuie inclusă cea mai bună estimare a investițiilor legate de tehnologia digitală generate de propunere/inițiativă.

În mod excepțional, atunci când este necesar pentru punerea în aplicare a propunerii/inițiativei, creditele de la rubrica 4 ar trebui prezentate la linia desemnată.

Creditele de la rubricile 1-3 ar trebui reflectate drept „Cheltuieli de politică IT pentru programele operaționale”. Aceste cheltuieli se referă la bugetul operațional care trebuie utilizat pentru reutilizarea/cumpărarea/dezvoltarea platformelor/instrumentelor IT direct legate de punerea în aplicare a inițiativei și pentru investițiile asociate acestora (de exemplu licențe, studii, stocarea datelor etc.). Informațiile prezentate în acest tabel ar trebui să fie coerente cu detaliile prezentate la secțiunea 4 „Dimensiunile digitale”.

TOTAL credite pentru componenta digitală și IT	Anul **2028**	Anul **2029**	Anul **2030**	Anul **2031**	Anul **2032**	Anul **2033**	Anul **2034**	**TOTAL CFM 2028-2034**
RUBRICA 4								
Cheltuieli IT (corporative)	0	0	0	0	0	0	0	**0**
Subtotal de la RUBRICA 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
În afara RUBRICII 4								
Cheltuieli de politică IT pentru programele operaționale	0	0	0	0	0	0	0	**0**
Subtotal în afara RUBRICII 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
TOTAL	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

3.2.6. Compatibilitatea cu cadrul financiar multianual actual

Propunerea/inițiativa:

– ☒ poate fi finanțată integral prin realocarea creditelor în cadrul rubricii relevante din cadrul financiar multianual (CFM)

Fără a aduce atingere negocierilor privind următorul CFM, creditele alocate agenției începând cu 2028 vor fi compensate prin redistribuiri de la programele din CFM 2028-2034. În cazul în care este necesară o reducere compensatorie, resursele alocate agenției, precum și fluxurile și sursele de finanțare ale acestora ar putea necesita o revizuire.

– ☐ necesită utilizarea marjei nealocate din cadrul rubricii corespunzătoare din CFM și/sau utilizarea instrumentelor speciale, astfel cum sunt definite în Regulamentul privind CFM

– ☐ necesită revizuirea CFM

3.2.7. Contribuțiile terților

Propunerea/inițiativa:

– ☒ nu prevede cofinanțare din partea terților

– ☐ prevede cofinanțare din partea terților, estimată mai jos:

Credite în milioane EUR (cu trei zecimale)

	Anul **2028**	Anul **2029**	Anul **2030**	Anul **2031**	Total
A se preciza organismul care asigură cofinanțarea					
TOTAL credite cofinanțate					

3.2.8. Estimarea resurselor umane și utilizarea creditelor necesare în cadrul unei agenții descentralizate

Cerințe privind personalul suplimentar (unități echivalent normă întreagă)

Agenția: ENISA	Anul **2028**	Anul **2029**	Anul **2030**	Anul **2031**	Anul **2032**	Anul **2033**	Anul **2034**
Agenți temporari (gradele AD)	5	11	17	19	19	19	19
Agenți temporari (gradele AST)	4	7	11	12	12	12	12
Subtotal agenți temporari (AD+AST)	***9***	***18***	***28***	***31***	***31***	***31***	***31***
Agenți contractuali	22	44	66	74	74	74	74
Experți naționali detașați	4	8	11	13	13	13	13
Subtotal agenți contractuali și experți naționali detașați	26	52	77	87	87	87	87
TOTAL personal	35	70	105	118	118	118	118

Credite acoperite de contribuția de la bugetul UE în milioane EUR (cu trei zecimale)

Agenția: ENISA	Anul **2028**	Anul **2029**	Anul **2030**	Anul **2031**	Anul **2032**	Anul **2033**	Anul **2034**	**TOTAL 2028-2034**
Titlul 1: Cheltuieli cu personalul	4,488	8,466	12,507	13,648	10,584	10,012	9,537	**87,766**
Titlul 2: Cheltuieli cu infrastructura și cheltuieli operaționale								
Titlul 3: Cheltuieli operaționale	16,413	11,588	11,528	11,788	11,613	11,613	11,113	**85,240**
TOTAL credite acoperite de bugetul UE	**20,901**	**20,054**	**24,035**	**25,437**	**22,197**	**21,625**	**21,151**	**155,4**

Credite acoperite de taxe, dacă este cazul, în milioane EUR (cu trei zecimale)

Agenția: ENISA	Anul 2028	Anul 2029	Anul 2030	Anul 2031	Anul 2032	Anul 2033	Anul 2034	TOTAL 2028-2034
Titlul 1: Cheltuieli cu personalul		0,510	1,043	1,539	4,604	5,176	5,650	**18,522**
Titlul 2: Cheltuieli cu infrastructura și cheltuieli operaționale								**0,000**
Titlul 3: Cheltuieli operaționale								**0,000**
TOTAL credite acoperite de taxe	**0,000**	**0,510**	**1,043**	**1,539**	**4,604**	**5,176**	**5,650**	**18,522**

Prezentare generală/sinteză a resurselor umane și a creditelor (în milioane EUR) necesare pentru propunere/inițiativă în cadrul unei agenții descentralizate

Agenția: ENISA	Anul 2028	Anul 2029	Anul 2030	Anul 2031	Anul 2032	Anul 2033	Anul 2034	TOTAL 2028-2034
Agenți temporari (AD+AST)	9	18	28	31	31	31	31	*31*
Agenți contractuali	22	44	66	74	74	74	74	74
Experți naționali detașați	4	8	11	13	13	13	13	13
Total personal	35	70	105	118	118	118	118	**118**
Credite acoperite de bugetul UE	**20,901**	**20,054**	**24,035**	**25,437**	**22,197**	**21,625**	**21,151**	**155,4**
Credite acoperite de taxe (dacă este cazul)	**0,000**	**0,510**	**1,043**	**1,539**	**4,604**	**5,176**	**5,650**	**18,522**
Credite cofinanțate (dacă este cazul)	0,000	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**
TOTAL credite	**20,901**	**20,564**	**25,078**	**26,976**	**26,801**	**26,801**	**26,801**	**173,922**

3.3. Impactul estimat asupra veniturilor

– ☒ Propunerea/inițiativa nu are impact financiar asupra veniturilor.

– ☐ Propunerea/inițiativa are următorul impact financiar:

  – ☐ asupra resurselor proprii

  – ☐ asupra altor venituri

– ☐ vă rugăm să precizați dacă veniturile sunt alocate unor linii de cheltuieli

milioane EUR (cu trei zecimale)

Linia bugetară pentru venituri:	Credite disponibile pentru exercițiul financiar în curs	Impactul propunerii/inițiativei[105]						
		Anul **2028**	Anul **2029**	Anul **2030**	Anul **2031**	Anul **2032**	Anul **2033**	Anul **2034**
Articolul …….								

Pentru veniturile alocate, a se preciza linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate).

Alte observații (de exemplu, metoda/formula utilizată pentru calcularea impactului asupra veniturilor sau orice alte informații).

Mecanismele de taxare sunt legate de trei domenii de activitate ale ENISA:

- Taxe legate de autorizarea furnizorilor în cadrul sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică.

Taxele legate de această activitate vor fi stabilite într-un act de punere în aplicare, în urma adoptării Regulamentului revizuit privind securitatea cibernetică. Cu toate acestea, pentru a putea estima investițiile necesare și costurile, calculele au fost efectuate utilizând un model existent într-un stat membru al UE[106]. Modelul include o plată unică și o taxă anuală.

Costuri fixe: 8,540 EUR

Taxa anuală: 800 EUR

Taxele sunt menite să refinanțeze costurile pentru această activitate specifică. Costurile au fost estimate la 1 064 600 EUR pe o perioadă de 5 ani. Costurile specifice ale activităților incluse în această cifră sunt legate de dezvoltarea și întreținerea sistemelor, inclusiv cheltuielile membrilor unui grup de lucru ad-hoc care ar urma să sprijine ENISA în dezvoltarea sistemelor (rambursarea cheltuielilor și plata raportorilor), misiunile la furnizorii de servicii de audit la fața locului și formarea evaluatorilor pentru a asigura aplicarea omogenă a sistemelor:

A) grupul de lucru ad-hoc ar costa 800 000 EUR

B) formarea a doi evaluatori pentru fiecare stat membru s-ar ridica la 129 600 EUR

C) auditarea unei entități per stat membru s-ar ridica la 135 000 EUR

(A + B + C) / 5 = 212 920 EUR costuri pe an

105 În ceea ce privește resursele proprii tradiționale (taxe vamale, cotizații pentru zahăr), sumele indicate trebuie să fie sume nete, și anume sumele brute după deducerea unei cote de 20 % pentru costurile de colectare.

106 Decizia RR-02: Lista de prețuri a serviciilor SNAS: https://www.snas.sk/storage/app/uploads/public/677/e79/e4c/677e79e4cac62903312474.pdf,

Propunerea prevedea o perioadă de tranziție și o investiție inițială în primii trei ani. În perioada de tranziție, costurile vor fi acoperite din bugetul UE, iar în anii 4 și 5 vom avea o acoperire de 50 %, anii 6 și 7 – aplicarea integrală a taxelor.

Anul	Taxe
2028	0
2029	0
2030	0
2031	106 460 (venituri)
2032	106 460 (venituri)
2033	212 920 (venituri)
2034	212 920 (venituri)

- Taxe legate de acoperirea costurilor de întreținere a unui sistem de certificare a securității cibernetice, adoptat în cadrul european de certificare a securității cibernetice (ECCF).

Taxele legate de această activitate vor fi stabilite într-un act de punere în aplicare, în urma adoptării Regulamentului revizuit privind securitatea cibernetică. Estimările costurilor de întreținere a unui sistem se bazează pe o analiză de piață, inclusă în evaluarea impactului propunerii de revizuire a Regulamentului privind securitatea cibernetică. Costurile totale ale activității pentru o perioadă de 5 ani sunt calculate la 5 600 000 EUR pentru costurile operaționale și la 7 100 000 EUR pentru ENI.

Costul anual al activităților de întreținere este calculat pe baza experienței actuale ca fiind de 200 000 EUR pe an de întreținere a unui sistem[107] și 2 ENI dedicate acestor activități (cu un cost anual de 125 887 EUR pe ENI), ținând seama de anul preconizat de adoptare a unor astfel de sisteme. Se așteaptă ca veniturile din aceste taxe să crească odată cu adoptarea fiecărui nou sistem și cu adoptarea treptată a unor astfel de sisteme. Până în prezent, a fost adoptat un sistem (EUCC) în cadrul ECCF și se preconizează că primele venituri din întreținerea sistemului respectiv vor fi obținute în 2029. Conform estimărilor, costurile vor fi acoperite până în 2032.

Veniturile estimate au fost calculate pe baza unor ipoteze specifice pentru fiecare sistem potențial cu privire la următoarele aspecte: adoptarea preconizată (numărul de certificate care urmează să fie eliberate), durata de valabilitate a fiecărui certificat și numărul de organisme active de evaluare a conformității. Se preconizează că adoptarea unui viitor sistem privind postura de securitate cibernetică va genera venituri substanțiale.

Anul	Venituri (procentul costurilor acoperite/plătite de la bugetul UE)

[107] Mai precis, întreținerea are în vedere 2 reuniuni cu prezență fizică cu experți pe an (100 000 EUR), costurile contractanților care sprijină elaborarea și revizuirea documentației justificative pentru sistem, adoptarea sistemelor de certificare, sprijinirea evaluărilor *inter pares* și punerea în aplicare a evaluărilor conformității (4 x 15 000 = 60 000 EUR). Costul include, de asemenea, partea operațională a platformei MIE și site-ul de certificare al ENISA (40 000 EUR).

2028 0

2029 250 000 (11 %/ - 1 350 000 EUR) – un sistem (EUCC)

2030 783 000 (29 %/ - 2 000 000 EUR) – trei sisteme (EUCC, ID Wallet, MSS)

2031 783 000 (25 %/ - 1 930 000 EUR) – trei sisteme (EUCC, ID Wallet, MSS)

2032 3 850 000 (122 %/ - 2 400 000 EUR) – cinci sisteme (EUCC, ID Wallet, MSS, EUCS, 5G)

2033 4 000 000 (126 %/ + 685 000 EUR) – șase sisteme (EUCC, ID Wallet, MSS, EUCS, 5G, Cyberposture)

2034 4 500 000 (141 %/ + 825 000 EUR) – șapte sisteme

Taxe legate de instrumentele de testare utilizate în sprijinul procedurilor de evaluare a conformității

Taxele legate de această activitate vor fi stabilite într-un act de punere în aplicare, în urma adoptării Regulamentului revizuit privind securitatea cibernetică. Cu toate acestea, pentru a indica costurile estimate și veniturile preconizate, calculele au fost efectuate pe baza estimărilor furnizate de ENISA și incluse în evaluarea impactului propunerii de revizuire a Regulamentului privind securitatea cibernetică. Costurile legate de sprijinul pentru activitățile de testare și evaluare sunt estimate la:

ENI: 4 pe an

Costuri operaționale: 800 000 pe an

Costuri totale: 6 500 000 M (5 ani); pe an: 1 300 000 EUR

Se preconizează că, pentru ENISA, vor avea loc primele investiții de la an la an, urmate de costuri de întreținere. Aceste costuri ar fi acoperite treptat de veniturile colectate din taxe.

Anul Venituri

2028 0

2029 260 000

2030 260 000

2031 650 000

2032 650 000

2033 975 000

2034 975 000

4. DIMENSIUNILE DIGITALE

4.1. Cerințe cu relevanță digitală

Descriere la nivel înalt a cerințelor privind relevanța digitală și a categoriilor conexe (date, digitalizarea și automatizarea proceselor, soluții digitale și/sau servicii publice digitale)

Trimiterea la cerință	**Descrierea cerinței**	**Actori afectați sau vizați de cerință**	**Procese la nivel înalt**	**Categorii**
Articolul 5 alineatul (1) litera (a) Sprijin pentru punerea în aplicare a legislației UE	(a) acordând asistență statelor membre în punerea în aplicare consecventă a politicii și a legislației Uniunii în materie de securitate cibernetică, inclusiv prin **emiterea de orientări tehnice și de rapoarte, prin furnizarea de consiliere și schimbul de bune practici și prin facilitarea schimbului de bune practici între autoritățile competente în această privință**;	- ENISA - statele membre	- prelucrarea datelor pentru a emite orientări tehnice, rapoarte, a oferi consiliere și a face schimb de bune practici și prin facilitarea schimbului de bune practici între autoritățile competente - facilitarea schimburilor de bune practici	Prelucrarea datelor Fluxul datelor
Articolul 5 alineatul (1) litera (b) Sprijin pentru punerea în aplicare a legislației UE	(b) sprijinind **schimbul de informații în cadrul sectoarelor și între acestea, în special în ceea ce privește sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555** și produsele cu elemente digitale care intră în domeniul de aplicare al Regulamentului (UE) 2024/2847**, prin furnizarea de bune practici și orientări privind instrumentele și procedurile disponibile**	- ENISA - sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555 - părțile interesate afectate de Regulamentul (UE) 2024/2847	furnizarea de bune practici și orientări privind instrumentele și procedurile disponibile pentru schimbul de informații	Prelucrarea datelor Fluxul datelor

Articolul 5 alineatul (1) litera (c) Sprijin pentru punerea în aplicare a legislației UE	(c) la cererea Comisiei, acordând asistență statelor membre prin furnizarea de sprijin, cum ar fi **orientări tehnice, inclusiv cu privire la măsurile de gestionare a riscurilor în materie de securitate cibernetică, instrumente de evaluare a maturității în materie de securitate cibernetică și manuale de răspuns la incidente**, adaptate sectoarelor enumerate în anexele I și II la Directiva (UE) 2022/2555, cu scopul de a facilita îmbunătățirea nivelului lor de maturitate în materie de securitate cibernetică și respectarea dreptului Uniunii în ceea ce privește securitatea cibernetică;	- Comisia Europeană - ENISA - sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555	Furnizarea de orientări tehnice	Prelucrarea datelor Fluxul datelor
Articolul 5 alineatul (1) litera (e)	(e) acordând asistență statelor membre și entităților relevante ale Uniunii în **elaborarea și promovarea politicilor de securitate cibernetică** legate de susținerea disponibilității și integrității generale a nucleului public al internetului deschis;	ENISA statele membre entități ale UE	Acordarea de asistență pentru elaborarea și promovarea politicilor în materie de securitate cibernetică	Prelucrarea datelor Fluxul datelor
Articolul 5 alineatul (1) litera (f) Sprijin pentru punerea în aplicare a legislației UE	(f) în conformitate cu Regulamentul (UE) 2024/2847, **furnizând consiliere și sprijin tehnic** cu privire la aspecte legate de punerea în aplicare și asigurarea respectării regulamentului respectiv	- ENISA - părțile interesate afectate de Regulamentul (UE) 2024/2847	Furnizarea de consiliere și sprijin tehnic necesită prelucrarea și schimbul de informații cu privire la cerințele de reglementare, la provocările legate de punerea în aplicare și orientările în materie de conformitate.	Prelucrarea datelor Fluxul datelor
Articolul 5 alineatul (1) litera (h)	(h) la cererea Comitetului european pentru protecția datelor, furnizând consiliere cu privire la punerea în aplicare a aspectelor specifice de securitate cibernetică ale politicii și legislației Uniunii legate de protecția datelor și a vieții private.	ENISA CEPD	Furnizarea de consiliere la cerere	Prelucrarea datelor Fluxul datelor

Articolul 5 alineatul (2) Contribuția la evaluările riscurilor în materie de securitate cibernetică la nivelul Uniunii	ENISA contribuie la evaluări coordonate ale riscurilor în materie de securitate cibernetică la nivelul Uniunii, inclusiv la cele efectuate în temeiul articolului 22 din Directiva (UE) 2022/2555.	ENISA Statele membre Publicul larg	Contribuția la evaluări coordonate ale riscurilor, care necesită prelucrarea datelor și fluxul de date	Prelucrarea datelor Fluxul datelor
Articolul 5 alineatul (3) ENISA emite orientări	ENISA **emite orientări** privind interoperabilitatea rețelelor și a sistemelor informatice utilizate pentru schimbul de informații, inclusiv în ceea ce privește centrele cibernetice transfrontaliere, astfel cum se menționează la articolul 6 alineatul (3) din Regulamentul (UE) 2025/38.	ENISA Statele membre	ENISA emite orientări	Prelucrarea datelor Fluxul datelor
Articolul 5 alineatul (5) Sprijin pentru Comisie	La **cererea Comisiei**, ENISA **furnizează expertiză, consiliere tehnică, informații sau analize sau desfășoară activități pregătitoare** cu privire la aspecte specifice legate de securitatea cibernetică, cu scopul de a contribui la elaborarea politicilor Comisiei și la monitorizarea punerii în aplicare a legislației Uniunii.	Comisia Europeană ENISA	Pregătirea și transmiterea informațiilor către Comisie	Prelucrarea datelor Fluxul datelor

Articolul 6 Consolidarea capacităților	ENISA oferă asistență prin furnizarea de cunoștințe și expertiză, bune practici etc.	ENISA Statele membre Entități ale UE Părți interesate din sectorul public și privat Autoritățile de supraveghere a pieței Membrii ECCG ECCC	Furnizarea de cunoștințe și expertiză	Prelucrarea datelor Fluxul datelor
Articolul 7 Acțiuni de sensibilizare și rezerva de talente	ENISA sprijină statele membre în eforturile lor de sensibilizare cu privire la politicile și legislația Uniunii în materie de securitate cibernetică și promovează vizibilitatea acestora **prin dezvoltarea de instrumente și orientări realizabile**. ENISA sprijină inițiativele care vizează creșterea rezervei europene de talente în materie de securitate cibernetică, în special prin coordonarea concursurilor.	ENISA Statele membre	Elaborarea de instrumente și orientări care pot fi puse în practică	Prelucrarea datelor
Articolul 8 alineatul (1) Cunoștințe și analize de piață	ENISA **efectuează și diseminează analize** ale principalelor tendințe ale pieței securității cibernetice, atât din perspectiva cererii, cât și din perspectiva ofertei, în special în ceea ce privește domeniile în care există sau sunt planificate sisteme europene de certificare a securității cibernetice, sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555 și categoriile de produse care intră sub incidența Regulamentului (UE) 2024/2847, inclusiv anexele III și IV la regulamentul respectiv.	ENISA Sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555 Categorii de produse reglementate de Regulamentul (UE) 2024/2847	Efectuarea și difuzarea de analize	Prelucrarea datelor Fluxul datelor

Articolul 8 alineatul (2) Cunoștințe și analize de piață	ENISA **efectuează și diseminează analize** ale tendințelor tehnologice în materie de securitate cibernetică, în special în ceea ce privește activitățile și entitățile care intră în domeniul de aplicare al Directivei (UE) 2022/2555 și produsele cu elemente digitale care intră în domeniul de aplicare al Regulamentului (UE) 2024/2847.	ENISA Publicul larg, părțile interesate în sensul Directivei (UE) 2022/2555 și al Regulamentului (UE) 2024/2847	Efectuarea și difuzarea de analize	Prelucrarea datelor Fluxul datelor
Articolul 8 alineatul (3) Cunoașterea pieței și sprijinirea ecosistemelor	ENISA consolidează cunoștințele și **diseminează consiliere tehnică și analize** cu privire la instrumente, cadre, standarde și bune practici de securitate cibernetică de ultimă generație.	ENISA Publicul larg	Diseminarea de consiliere tehnică și analize privind instrumente, cadre, standarde și bune practici de securitate cibernetică de ultimă generație.	Prelucrarea datelor Fluxul datelor
Articolul 9 Cooperarea internațională	ENISA contribuie prin analizarea rezultatelor exercițiilor internaționale și raportarea acestora către consiliul de administrație, facilitând schimbul de bune practici, oferind Comisiei expertiză și consiliere.	Publicul internațional ENISA Consiliul de administrație al ENISA Comisia Europeană	Analiza și raportarea; furnizarea de consiliere etc.	Prelucrarea datelor Fluxul datelor
Articolul 10 alineatele (2) și (3) Cooperare operațională	(2) ENISA este membră a rețelei de echipe CSIRT naționale instituite în temeiul articolului 15 alineatul (1) din Directiva (UE) 2022/2555 și **asigură secretariatul** rețelei CSIRT în temeiul articolului 15 alineatul (2) din	ENISA Echipele CSIRT [articolul 15 alineatul (1) din Directiva (UE) 2022/2555]. EU-CyCLONe [articolul 16	Facilitarea schimbului de informații, îndeplinirea sarcinilor de secretariat al rețelelor	Fluxul datelor Soluția digitală Serviciul public digital

	Directiva (UE) 2022/2555. (3) ENISA **asigură secretariatul** Rețelei europene a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe) în temeiul articolului 16 alineatul (2) al doilea paragraf din Directiva (UE) 2022/2555.	alineatul (2) din Directiva (UE) 2022/2555].		
Articolul 11 alineatul (1) litera (b) Conştientizarea situaţiei Articolul 12 Alerte timpurii	**emiterea de alerte timpurii** în conformitate cu articolul 12	Comisia Europeană ENISA Europol EU-CyCLONe Reţeaua CSIRT CERT-UE Entităţile enumerate în anexele I şi II la Directiva (UE) 2022/2555	Emiterea de alerte timpurii	Prelucrarea datelor Fluxul datelor Serviciul public digital
Articolul 10 alineatul (4) litera (b) Cooperare operaţională	(b) la cererea unuia sau mai multor state membre, **furnizarea de consiliere şi evaluări în legătură cu un anumit incident potenţial sau în curs sau cu o anumită ameninţare cibernetică**, inclusiv prin furnizarea de expertiză şi prin **facilitarea gestionării tehnice a unor astfel de incidente**, precum şi prin **sprijinirea schimbului voluntar de informaţii relevante şi de soluţii tehnice între statele membre;**	ENISA statele membre	Furnizarea de consiliere şi evaluări în legătură cu un anumit incident sau ameninţare cibernetică potenţial(ă) sau în curs; Facilitarea gestionării tehnice a unor astfel de incidente; Sprijinirea schimbului voluntar de informaţii şi soluţii tehnice relevante între statele membre	Prelucrarea datelor Fluxul datelor Servicii publice digitale

Articolul 10 alineatul (4) litera (c) Cooperare operațională	(c) analizarea vulnerabilităților, a amenințărilor și a incidentelor;	ENISA Statele membre	Colectarea datelor din surse publice și schimbul de date cu statele membre	Prelucrarea datelor Fluxul datelor
Articolul 10 alineatul (4) litera (d) Cooperare operațională	(d) la **cererea unuia sau mai multor state membre**, **oferind sprijin** în legătură cu anchetele tehnice *ex post* privind incidentele semnificative în înțelesul Directivei (UE) 2022/2555;	ENISA Statele membre	Analiză și sprijin ca răspuns la anchetele tehnice privind incidentele	Prelucrarea datelor Fluxul datelor
Articolul 10 alineatul (4) litera (e) Cooperare operațională	(e) contribuția la sprijinirea gestionării coordonate a incidentelor și a crizelor de securitate cibernetică de mare amploare la nivel operațional, în special prin **sprijinirea EU-CyCLONe în pregătirea rapoartelor către nivelul politic și prin facilitarea schimbului de informații în timp util între rețeaua CSIRT și EU-CyCLONe;**	ENISA EU-CyCLONe Rețeaua CSIRT	Analizarea datelor pentru a sprijini pregătirea rapoartelor; facilitarea schimbului de informații în timp util între rețele	Prelucrarea datelor Fluxul datelor Serviciul public digital
Articolul 10 alineatul (5) Cooperare operațională	La **cererea unui stat membru** sau a unei entități a Uniunii în cooperare cu CERT-UE, ENISA sprijină comunicarea publică coerentă cu privire la un incident sau o amenințare cibernetică.	ENISA Statele membre	Primirea cererii și comunicarea, dacă este necesar	Fluxul datelor

Articolul 10 alineatul (6) Cooperare operațională	ENISA **sprijină** cooperarea dintre statele membre și, prin intermediul CERT-UE, dintre entitățile Uniunii în ceea ce privește **implementarea instrumentelor de comunicații securizate.** ENISA utilizează, în cadrul rețelei CSIRT și al EU-CyCLONe, instrumente securizate de comunicații care sunt furnizate de entități juridice care nu sunt stabilite în țări terțe sau controlate de țări terțe sau de resortisanți ai țărilor terțe.	ENISA Comisia Europeană statele membre entități ale UE Rețeaua CSIRT EU-CyCLONe	Sprijinirea implementării unor instrumente de comunicare securizate și utilizarea unor astfel de instrumente în cadrul rețelei CSIRT și al EU-CyCLONe.	Soluția digitală Serviciul public digital
Articolul 11 alineatul (1) litera (a) Conștientizarea comună a situației în materie de securitate cibernetică	(a) **dezvoltă**, în cooperare cu EU-CyCLONe, rețeaua CSIRT, Comisia, CERT-UE, Europol și alte entități relevante ale Uniunii, **registre** de informații verificate și fiabile privind amenințările cibernetice, inclusiv tendințele în materie de incidente, tactici, tehnici și proceduri;	Comisia Europeană ENISA EU-CyCLONe Rețeaua CSIRT Europol entități ale UE CERT-UE	Dezvoltarea de registre	Fluxul digital Soluția digitală Serviciul public digital
Articolul 11 alineatul (1) literele (c)-(g) Conștientizarea comună a situației în materie de securitate cibernetică	Furnizarea de analize ad-hoc în timp util (unele la cerere); furnizarea de analize și consultanță tehnică; elaborarea raportul privind situația tehnică în cooperare cu alte entități; monitorizarea tendințelor și partajarea acestora	ENISA statele membre Comisia Europeană entități ale UE EU-CyCLONe Rețeaua CSIRT	Analiza datelor, schimbul de informații și furnizarea de rapoarte (unele la cerere)	Prelucrarea datelor Fluxul datelor

Articolul 11 alineatul (2) litera (a) Conștientizarea comună a situației în materie de securitate cibernetică	ENISA **efectuează analize** ale amenințărilor cibernetice, ale incidentelor, ale tendințelor, ale tehnologiilor emergente și ale impactului acestora, inclusiv o **analiză** periodică a sectoarelor enumerate în anexele I și II la Directiva (UE) 2022/2555 și a categoriilor de produse relevante care intră sub incidența Regulamentului (UE) 2024/2847;	ENISA Publicul larg	Analiza datelor pentru a furniza informații cu impact asupra securității cibernetice; raport periodic	Prelucrarea datelor Fluxul datelor
Articolul 11 alineatul (2) litera (b) Conștientizarea comună a situației în materie de securitate cibernetică	ENISA **emite, în cooperare cu Comisia și, după caz, cu rețeaua CSIRT, consiliere, orientări și bune practici** pentru securitatea rețelelor și a sistemelor informatice, în special pentru securitatea infrastructurilor care sprijină sectoarele enumerate în anexele I și II la Directiva (UE) 2022/2555;	Comisia Europeană CERT-UE Rețeaua CSIRT Publicul larg	Emiterea de consiliere, orientări și bune practici	Prelucrarea datelor Fluxul datelor
Articolul 11 alineatul (2) punctul (c) Conștientizarea comună a situației în materie de securitate cibernetică	ENISA efectuează **analize strategice pe termen lung ale amenințărilor cibernetice** și incidentelor, pentru a **identifica** tendințele emergente și a contribui la prevenirea incidentelor.	ENISA Publicul larg	Analiza datelor și identificarea amenințărilor emergente	Prelucrarea datelor
Articolul 11 alineatul (3) Conștientizarea comună a situației în materie de securitate cibernetică	ENISA poate **face publice analizele**, consilierea, orientările, bunele practici și rapoartele menționate la alineatul (2), de comun acord cu entitățile contribuitoare menționate la alineatul (2).	ENISA Publicul larg	Punerea informațiilor la dispoziția publicului	Fluxul datelor Serviciul public digital

Articolul 13 alineatul (2) Sprijin pentru răspunsul la incidente	(2) La cererea Comisiei sau a EU-CyCLONe, ENISA, cu sprijinul rețelei CSIRT și cu aprobarea statului membru în cauză, **revizuiește și evaluează incidentele de securitate cibernetică semnificative** sau incidentele de securitate cibernetică de mare amploare în conformitate cu articolul 21 din Regulamentul (UE) 2025/38.	Comisia Europeană ENISA EU-CyCLONe Rețeaua CSIRT Statele membre	Revizuirea și evaluarea incidentelor de securitate cibernetică semnificative	Prelucrarea datelor
Articolul 14 alineatul (2) Exerciții de securitate cibernetică la nivelul Uniunii	(2) ENISA **menține un registru** al învățămintelor desprinse în urma exercițiilor menționate la alineatul (1) și recomandă statelor membre și, după caz, entităților Uniunii modul în care pot fi puse în aplicare în mod eficace și eficient învățămintele desprinse.	ENISA statele membre entități ale UE	Menținerea unui registru	Prelucrarea datelor Soluția digitală Serviciul public digital
Articolul 14 Exerciții de securitate cibernetică la nivelul Uniunii	La primirea cererilor din partea EU-CyCLONe, a Comisiei, a statelor membre sau a CERT-UE, ENISA organizează exerciții de securitate cibernetică sau contribuie la organizarea acestora. ENISA sprijină Comisia în elaborarea unui program anual continuu de exerciții de securitate cibernetică la nivelul Uniunii.	ENISA Comisia statele membre entități ale UE CERT-UE	Primirea cererilor de organizare sau de sprijinire a organizării de exerciții	Fluxul datelor Prelucrarea datelor

Articolul 15 Furnizarea de instrumente și platforme	(1) **ENISA instituie, furnizează, operează, întreține și actualizează, după caz, instrumente tehnice operaționale, inclusiv platforme** legate de securitatea cibernetică la nivelul Uniunii, în special platforma unică de raportare a incidentelor instituită în temeiul articolului 16 alineatul (1) din Regulamentul (UE) 2024/2847 [și punctul unic de intrare instituit în temeiul articolului 23a din Directiva (UE) 2022/2555], precum și instrumente de testare pentru a sprijini punerea în aplicare a procedurilor de evaluare a conformității în conformitate cu legislația relevantă a Uniunii. (2) După caz, în sensul alineatului (1), **ENISA cooperează și face schimb de informații** cu rețeaua CSIRT și, după caz, cu autoritățile de supraveghere a pieței.	ENISA Rețeaua CSIRT Publicul larg Autoritățile de supraveghere a pieței	ENISA instituie, furnizează, operează, întreține și actualizează, după caz, instrumente tehnice operaționale, cum ar fi platformele	Soluția digitală Serviciul public digital Fluxul datelor
Articolul 16 alineatul (2) Servicii de gestionare a vulnerabilităților	(a) întreținerea bazei de date europene a vulnerabilităților instituite în temeiul articolului 12 alineatul (2) din Directiva (UE) 2022/2555; (b) furnizarea de servicii de gestionare a vulnerabilităților către **părțile interesate**, pe baza bazei de date europene a vulnerabilităților și utilizând informațiile relevante aflate la dispoziția ENISA; (c) după caz, inițierea unei cooperări structurate cu **organizații** care furnizează programe, registre sau baze de date similare cu baza de date europeană a vulnerabilităților; (d) sprijinirea activă a **echipelor CSIRT** desemnate drept coordonatori în temeiul articolului 12 alineatul (1) din Directiva (UE) 2022/2555 în ceea ce privește gestionarea	ENISA Echipele CSIRT naționale Rețeaua CSIRT Autoritățile naționale competente Industria Comunitatea de cercetare Publicul larg Actori internaționali care furnizează programe, registre sau baze de date	Furnizarea de servicii de gestionare a vulnerabilităților; inițierea unei cooperări structurate, după caz; cooperarea cu părțile interesate	Soluția digitală Serviciul public digital Fluxul datelor

	divulgării coordonate a vulnerabilităților care pot avea un impact semnificativ asupra entităților din mai multe state membre; (e) dezvoltarea și menținerea metodologiilor și a mecanismelor de guvernanță pentru identificarea vulnerabilităților și divulgarea coordonată, **în cooperare cu autoritățile naționale competente, echipele CSIRT, industria și comunitatea de cercetare.**			
Articolul 17 Certificarea securității cibernetice Articolul 18 Standardizare, specificații tehnice și orientări	Articolul 17 alineatul (1) (a) **pregătirea propunerilor de sisteme europene de certificare a securității cibernetice („propuneri de sisteme")** pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate și postura de securitate cibernetică a entităților și specificațiile tehnice aferente în conformitate cu articolul 74; (b) **întreținerea sistemelor europene de certificare a securității cibernetice** adoptate în conformitate cu articolul 75, inclusiv în vederea unei posibile revizuiri a sistemelor europene de certificare a securității cibernetice adoptate în conformitate cu articolul 76; (c) promovarea adoptării sistemelor adoptate și menținerea unui site dedicat care să ofere informații privind sistemele europene de certificare a securității cibernetice, certificatele europene de securitate cibernetică și declarațiile de conformitate UE în conformitate cu articolul 79 și să le facă publice; Articolul 17 alineatul (2) (e) **elaborarea** de modele de dispoziții care să	ENISA Publicul larg	Analizarea datelor și schimbul de fluxuri de date cu Comisia și cu alte părți interesate; pregătirea propunerii de sistem de certificare; menținerea site-ului ENISA	Prelucrarea datelor Fluxuri de date Serviciul public digital

	fie menționate în sistemele europene de certificare a securității cibernetice („propuneri de sisteme”) pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate și postura de securitate cibernetică a entităților, în conformitate cu articolul 81 alineatul (5). Articolul 18 (1) ENISA elaborează proiecte de specificații tehnice și orientări pentru a sprijini punerea în aplicare a legislației Uniunii în domeniul securității cibernetice. (2) ENISA **monitorizează, participă și conduce activitățile de dezvoltare a standardizării** la nivelul Uniunii și, în conformitate cu articolul 9, la nivel internațional. (3) ENISA sprijină dezvoltarea și evaluarea algoritmilor criptografici. În cazul în care un algoritm criptografic evaluat este evaluat pozitiv, ENISA cooperează, în conformitate cu Regulamentul (UE) nr. 1025/2012, cu organismele europene de standardizare pentru a sprijini standardizarea acestuia. (4) ENISA **furnizează Comisiei și ECCG expertiză tehnică** cu privire la standardele sau specificațiile tehnice adecvate în sprijinul politicilor Uniunii legate de securitatea cibernetică, în special al Regulamentului (UE) 2024/2847, inclusiv pentru legislația de armonizare a Uniunii în domeniul securității cibernetice și pentru sistemele europene de certificare a securității cibernetice în temeiul			

	articolului 81 alineatul (1) litera (d). (5) ENISA asistă Comisia la evaluarea proiectelor de standarde armonizate pentru a sprijini punerea în aplicare a legislației de armonizare a Uniunii în domeniul securității cibernetice.			
Articolul 19 – Cadrul european de competențe în materie de securitate cibernetică	ENISA **elaborează și pune la dispoziția publicului un cadru european de competențe în materie de securitate cibernetică („ECSF”)**. Înainte de a pune ECSF la dispoziția publicului sau de a-l actualiza în temeiul alineatului (4), ENISA **consultă Comisia.** Utilizarea ECSF este **voluntară pentru entitățile publice și private**. ENISA poate **consulta părțile interesate** în dezvoltarea și adoptarea ECSF.	ENISA Comisia Publicul larg Statele membre Entități ale UE Părți interesate din sectorul public și privat	Întreținerea ECSF; consultarea părților interesate; adoptarea ECSF	Prelucrarea datelor Fluxul datelor Soluția digitală
Articolele 20-23 – Sisteme europene de atestare individuală a competențelor în materie de securitate cibernetică	ENISA **elaborează, adoptă și întreține sisteme europene de atestare individuală a competențelor în materie de securitate cibernetică**. Utilizarea sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică este **voluntară pentru organismele publice naționale și entitățile private**, cu excepția cazului în care se prevede altfel în dreptul intern. Înainte de a iniția un nou sistem european de atestare individuală a competențelor în materie de securitate cibernetică, ENISA **consultă Comisia**. ENISA adoptă un astfel de sistem numai în urma unui **aviz pozitiv din partea Comisiei**. Atunci când pregătește un sistem european de atestare individuală a competențelor în materie de securitate cibernetică, ENISA poate **consulta părțile interesate relevante.**	ENISA Comisia Publicul larg Statele membre Entități ale UE Părțile interesate din sectorul public și privat (care contribuie la dezvoltarea unui sistem de atestare; solicitanți și furnizori europeni de atestate individuale de competențe în materie de securitate cibernetică, inclusiv evaluatori)	Dezvoltarea și întreținerea sistemelor; consultarea părților interesate; procesarea cererilor; emiterea deciziilor; menținerea unui site	Prelucrarea datelor Fluxul datelor Soluția digitală Serviciul public digital

	ENISA asigură o **cooperare strânsă cu statele membre** pe tot parcursul elaborării sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică. Furnizorii de atestate autorizați **evaluează dacă persoanele îndeplinesc cerințele** unui sistem de atestare europeană individuală a competențelor în materie de securitate cibernetică și, în cazul în care aceste cerințe sunt îndeplinite, eliberează atestate europene individuale de competențe în materie de securitate cibernetică. ENISA **oferă orientări evaluatorilor și asigură formarea obligatorie a acestora** în ceea ce privește cerințele și metodele de evaluare incluse în sistemul european de atestare individuală a competențelor în materie de securitate cibernetică, astfel cum se menționează la articolul 20 alineatul (3) litera (b). Entitățile care doresc să devină furnizori de atestate autorizați sau să își reînnoiască autorizația **(„solicitanții") trebuie să depună o cerere** la ENISA. Furnizorii de atestate autorizați se asigură că, **la cererea persoanei,** atestatele electronice aferente atestatelor europene individuale de competențe în materie de securitate cibernetică sunt emise ca atestate electronice ale atributelor într-un format care poate fi stocat în portofelele europene pentru identitatea digitală prevăzute în Regulamentul (UE) nr. 910/2014. Solicitanții și furnizorii de atestate autorizați permit **ENISA să efectueze evaluări** în cadrul procesului inițial de depunere a cererilor, de			

	menținere a autorizației sau de reînnoire a acesteia și să partajeze toate informațiile relevante pentru a se asigura că cerințele prevăzute la alineatele (3) și (4) și obligațiile prevăzute la alineatul (5) sunt îndeplinite sau continuă să fie îndeplinite în conformitate cu articolul 22 alineatul (2). Furnizorii de atestate autorizați **informează imediat ENISA** în cazul în care oricare dintre cerințele enumerate la alineatul (3) nu mai este îndeplinită sau în cazul în care apare orice îndoială că cerințele respective nu sunt îndeplinite, inclusiv în ceea ce privește independența evaluatorilor. Solicitanții **plătesc ENISA o taxă** pentru evaluarea cererii lor. Furnizorii de atestate autorizați **plătesc ENISA o taxă** pentru menținerea autorizației lor. **ENISA evaluează** dacă cerințele prevăzute la articolul 21 alineatele (3) și (4) și obligațiile prevăzute la articolul 21 alineatul (5) sunt îndeplinite sau continuă să fie îndeplinite de solicitanți și de furnizorii de atestate autorizați. După examinarea unei cereri în conformitate cu cerințele prevăzute la articolul 21 alineatele (3) și (4), **ENISA poate emite o decizie**. **ENISA poate modifica, suspenda sau revoca astfel de decizii**. **ENISA menține și actualizează periodic un site dedicat** care oferă informații publice cu privire la: (a) ECSF, inclusiv cadrul și			

	calendarul de actualizare a acestuia; (b) sistemele europene de atestare individuală a competențelor în materie de securitate cibernetică, progresele înregistrate de acestea și termenele pentru dezvoltarea lor; (c) taxele asociate fiecărui sistem european de atestare individuală a competențelor în materie de securitate cibernetică adoptat în temeiul articolului 47 din prezentul regulament; (d) costul orientativ al unui atestat european individual de competențe în materie de securitate cibernetică în conformitate cu articolul 20 alineatul (4); (e) lista furnizorilor de atestate autorizați.			

Articolul 25 Componența consiliului de administrație	**Numirea membrilor** consiliului de administrație al ENISA.	ENISA Comisia Europeană statele membre	Numirea membrilor	Fluxul datelor Prelucrarea datelor
Articolul 28 alineatul (1) Funcțiile consiliului de administrație Articolul 30 Comitetul executiv	b. adoptă proiectul de document unic de programare al ENISA menționat la articolul 44, înainte de **transmiterea acestuia Comisiei spre avizare**; (f) **evaluează** și adoptă raportul anual consolidat privind activitățile ENISA, care include conturile ENISA și descrierea modului în care aceasta și-a atins indicatorii de performanță, **transmite Parlamentului European, Consiliului, Comisiei și Curții de Conturi Europene, până la data de 1 iulie a anului următor, atât raportul anual, cât și evaluarea** acestuia; face public raportul anual; (i) asigură adoptarea de **măsuri subsecvente adecvate pentru a da curs constatărilor** și recomandărilor care decurg din rapoartele de audit și evaluările interne sau externe, precum și din investigațiile desfășurate de Oficiul European de Luptă Antifraudă („OLAF”) și de Parchetul European („EPPO”);	ENISA Comisia Europeană Parlamentul European Consiliul UE Curtea de Conturi Statele membre Publicul larg	Transmiterea DUP către Comisie în vederea obținerii unui aviz; Evaluarea și adoptarea raportului anual consolidat privind activitățile ENISA, inclusiv conturile și o descriere a modului în care ENISA și-a îndeplinit indicatorii de performanță, prezentarea atât a raportului anual, cât și a evaluării; Măsuri subsecvente întreprinse în urma constatărilor	Fluxul datelor Prelucrarea datelor

Articolul 31 alineatul (8) Numirea, revocarea și prelungirea mandatului	**Consiliul de administrație informează Parlamentul European** în legătură cu intenția sa de a prelungi mandatul directorului executiv în conformitate cu alineatul (6). În cursul perioadei de trei luni care precedă prelungirea mandatului său, directorul executiv, dacă este invitat, face o declarație în fața comisiei relevante a Parlamentului European și răspunde întrebărilor deputaților.	ENISA Consiliul de administrație al ENISA Parlamentul European	Consiliul de administrație informează Parlamentul European.	Fluxul datelor
Articolul 32 alineatul (3) Atribuțiile și responsabilitățile directorului executiv Articolul 32 alineatul (5)	(3) **Directorul executiv prezintă Parlamentului European, atunci când este invitat să facă acest lucru, un raport** privind modul în care și-a îndeplinit sarcinile. Consiliul îi poate cere directorului executiv să prezinte un raport referitor la modul în care și-a îndeplinit sarcinile. Elaborarea de strategii privind proiectele de planuri bugetare și de documente strategice.	Directorul executiv al ENISA Parlamentul European	Raportările privind performanța	Fluxul datelor Prelucrarea datelor
Articolul 35 alineatele (5) și (6) Grupul consultativ al ENISA	(5) Grupul consultativ al ENISA **acordă consiliere ENISA** în exercitarea atribuțiilor sale, cu excepția aplicării dispozițiilor titlurilor III, IV și V din prezentul regulament. Acesta acordă consiliere în special directorului executiv în ceea ce privește elaborarea unei propuneri de program anual de activitate al ENISA și asigurarea comunicării cu părțile interesate relevante referitor la aspecte legate de programul anual de activitate. (6) Grupul consultativ al ENISA **informează periodic consiliul de administrație** despre activitățile sale.	ENISA Membrii grupului consultativ al ENISA Consiliul de administrație al ENISA Directorul executiv al ENISA	Oferă consiliere și informații cu privire la activitățile sale	Prelucrarea datelor Fluxul datelor

Articolele 36-43 Comisia pentru soluționare a contestațiilor	ENISA instituie o **comisie pentru soluționarea contestațiilor** printr-o decizie a consiliului de administrație. Comisia pentru soluționarea contestațiilor este alcătuită dintr-un președinte și alți trei membri. Fiecare membru al comisiei pentru soluționarea contestațiilor are un supleant. Supleantul reprezintă membrul în absența acestuia. Consiliul de administrație **numește președintele, ceilalți membri și supleanții acestora** de pe o **listă de candidați calificați stabilită de Comisie**. Lista candidaților calificați este valabilă timp de patru ani. Valabilitatea acestei liste poate fi prelungită de consiliul de administrație cu perioade suplimentare de patru ani, la propunerea Comisiei. În cazul în care comisia pentru soluționarea contestațiilor consideră că natura cauzei o impune, ea poate solicita **consiliului de administrație să numească până la doi alți membri și supleanți** ai acestora de pe lista menționată la alineatul (3). Comisia pentru soluționarea contestațiilor își adoptă **propriul regulament de procedură și îl face public**. Dacă, pentru unul dintre motivele menționate la alineatul (1) sau pentru orice alt motiv, un membru al unei comisii pentru soluționarea contestațiilor consideră că nu trebuie să participe la procedura de soluționare a contestațiilor, acesta **informează comisia pentru soluționarea contestațiilor în mod corespunzător**.	ENISA Consiliul de administrație al ENISA Comisia Comisia pentru soluționarea contestațiilor în sensul articolului 36 din propunerea CSA2 Solicitanți (persoane juridice care doresc să devină furnizori de atestate autorizați, să își mențină sau să își reînnoiască autorizația)	Emiterea deciziilor pe baza contestațiilor Soluționarea contestațiilor Elaborarea și publicarea regulamentului de procedură Fluxuri de informații	Prelucrarea datelor Fluxul datelor Serviciul public digital

	Comisia pentru soluționare a contestațiilor **hotărăște măsurile aplicabile** în cazurile enumerate la alineatele (2) și (3) fără participarea membrului în cauză. În scopul luării acestei decizii, membrul în cauză este înlocuit în cadrul comisiei pentru soluționarea contestațiilor de către supleantul său. O contestație formulată în temeiul alineatului (1) face obiectul unei revizuiri preliminare în conformitate cu articolul 41 înainte de a fi supusă examinării comisiei pentru soluționarea contestațiilor. Solicitanții în sensul articolului 21 alineatul (3) pot introduce o **contestație împotriva: unei decizii a ENISA** care le-a fost adresată, în temeiul articolului 22 alineatul (3), cu privire nerespectarea de către ENISA a obligației de a acționa în ceea ce privește o cerere depusă de aceștia la ENISA în termenele aplicabile prevăzute la articolul 22 alineatul (4). În cazul menționat la alineatul (1) litera (a), contestația, împreună cu expunerea de motive a acesteia, **se depune în scris**, în conformitate cu regulamentul de procedură menționat la articolul 36 alineatul (5), în termen de două luni de la notificarea deciziei către solicitantul în cauză sau, în absența acesteia, de la data la care solicitantul a luat cunoștință de decizie. În cazul menționat la alineatul (1) litera (b), contestația **se introduce în scris la ENISA**, în conformitate cu regulamentul de procedură menționat la articolul 36 alineatul (5), în termen de două luni de la data expirării termenului prevăzut la articolul 22 alineatul (4).			

	Dacă ENISA consideră contestația admisibilă și bine întemeiată, aceasta **revine asupra deciziei sau abținerii de a acționa** menționate la articolul 40 alineatul (1). În cazul în care ENISA nu revine asupra deciziei în termen de o lună de la primirea contestației, aceasta **decide imediat dacă suspendă aplicarea deciziei sale și înaintează contestația comisiei pentru soluționarea contestațiilor**. **Comisia pentru soluționarea contestațiilor decide**, în termen de trei luni de la data introducerii contestației, dacă admite sau respinge contestația respectivă. Atunci când examinează o contestație, comisia pentru soluționarea contestațiilor acționează în termenele stabilite în regulamentul său de procedură. Comisia pentru soluționarea contestațiilor **invită părțile la procedura de contestare, ori de câte ori este necesar, să prezinte, în termenele stabilite, observații cu privire la notificările făcute de comisia pentru soluționarea contestațiilor sau la comunicările altor părți la procedura de contestare**. Părțile la procedurile de contestație au dreptul să își **prezinte oral argumentele**. În cazul în care comisia pentru soluționarea contestațiilor constată că motivele de introducere a unei contestații sunt întemeiate, aceasta **înaintează cazul către ENISA.** ENISA **ia decizia finală** în conformitate cu constatările comisiei pentru soluționarea contestațiilor și **furnizează o expunere de motive aferentă deciziei respective**. ENISA **informează în**			

	consecință părțile la procedura de contestare. Acțiunile în anulare împotriva deciziilor ENISA adoptate în temeiul articolului 22 alineatul (3) sau acțiunile în constatarea abținerii de a acționa în termenele aplicabile în temeiul articolului 22 alineatul (4) pot **fi introduse în fața Curții de Justiție a Uniunii Europene**, după epuizarea procedurii de soluționare a contestațiilor în cadrul ENISA prevăzute la articolele 39-42 sau în cazul abținerii de a acționa în termenul aplicabil în temeiul articolului 41 alineatul (2). ENISA **ia toate măsurile necesare pentru a aduce la îndeplinire** hotărârea Curții de Justiție a Uniunii Europene.			
Articolul 44 Documentul unic de programare	(2) În fiecare an, directorul executiv elaborează un proiect de document unic de programare, astfel cum se menționează la alineatul (1), cu planificarea corespunzătoare a resurselor financiare și umane în conformitate cu articolul 32 din Regulamentul delegat (UE) 2019/715 al Comisiei și luând în considerare orientările stabilite de Comisie. (3) Până la data de 30 noiembrie a fiecărui an, consiliul de administrație adoptă documentul unic de programare menționat la alineatul (1), ținând seama de avizul Comisiei menționat la articolul 32 alineatul (7) din Regulamentul delegat (UE) 2019/715. În cazul în care consiliul de administrație decide să nu ia în considerare vreun element din avizul Comisiei, furnizează o justificare detaliată a deciziei respective. Până la data de 31 ianuarie a anului următor, consiliul de administrație transmite documentul unic de programare Parlamentului European, Consiliului	Directorul executiv al ENISA Consiliul de administrație al ENISA Comisia Europeană Parlamentul European Consiliul	Elaborarea, adoptarea și transmiterea unui document unic de programare în fiecare an	Fluxul datelor

	și Comisiei, precum și orice versiune actualizată ulterior a documentului respectiv.			
Articolul 45 Întocmirea bugetului ENISA	(4) **Comisia transmite proiectul de estimare autorității bugetare**, împreună cu proiectul de buget general al Uniunii. Proiectul de buget estimativ este, de asemenea, pus la dispoziția ENISA.	ENISA Comisia Europeană	Schimbul de informații	Fluxul datelor
Articolul 47 Taxe	În ceea ce privește activitățile sistemelor europene de atestare individuală prevăzute la articolul 22 alineatul (1), **se percep următoarele taxe** solicitanților în sensul articolului 21 alineatul (3) sau furnizorilor de atestate autorizați pentru a contribui la acoperirea costurilor totale ale activităților desfășurate de ENISA: a. eliberarea autorizațiilor în urma examinării cerințelor prevăzute la articolul 21 alineatele (3) și (4), inclusiv efectuarea de evaluări; b. menținerea anuală a autorizației; c. reînnoirea autorizațiilor pentru furnizorii de atestate europene individuale de competențe în materie de securitate cibernetică, inclusiv efectuarea de evaluări. În ceea ce privește certificarea, **se percep următoarele taxe organismelor de evaluare a conformității** pentru întreținerea sistemelor europene de certificare a securității cibernetice	Comisia ENISA Furnizori de atestare Organisme de evaluare a conformității	Informații referitoare la prelucrare; plata taxelor; raportarea cu privire la taxe	Prelucrarea datelor Fluxul datelor

	în temeiul cărora sunt eliberate certificatele europene de securitate cibernetică, în special: o taxă anuală pentru participarea la un sistem european de certificare a securității cibernetice; o taxă pentru eliberarea de certificate europene de securitate cibernetică în cadrul sistemelor europene de certificare a securității cibernetice. Taxele menționate la litera (b) se percep atunci când organismul de evaluare a conformității transmite ENISA certificatele europene de securitate cibernetică în vederea publicării pe site-ul său în temeiul articolului 79. **Comisia adoptă acte de punere în aplicare** prin care stabilește norme detaliate privind taxele percepute de ENISA. ENISA include un **raport privind taxele percepute și impactul acestora asupra bugetului agenției** în cadrul procedurii de prezentare a conturilor.			
Articolul 48 Articolul 49 Implicațiile bugetare	Articolul 48 (3) În fiecare an, directorul executiv **transmite autorității bugetare toate informațiile** relevante pentru constatările procedurilor de evaluare. Articolul 49 (1) Contabilul ENISA **trimite conturile provizorii contabilului Comisiei și Curții de Conturi pentru exercițiul financiar** (anul N) până la data de 1 martie a următorului exercițiu financiar (anul N + 1). (2) Până la data de 1 martie a anului N + 1, contabilul autorității **comunică, de asemenea, informațiile contabile necesare în scopuri de consolidare către contabilul Comisiei**, în	ENISA Consiliul de administrație al ENISA Comisia Europeană Consiliul Parlamentul European	Prelucrarea și schimbul de informații privind bugetul ENISA.	Prelucrarea datelor Fluxul datelor

	modul și formatul solicitat de aceasta din urmă. (3) Până la data de 31 martie a anului N + 1, **ENISA trimite raportul privind gestiunea bugetară și financiară pentru anul N Parlamentului European, Consiliului, Comisiei** și Curții de Conturi. (4) **După primirea observațiilor formulate de Curtea de Conturi cu privire la conturile provizorii ale ENISA pentru anul N**, contabilul agenției întocmește conturile finale ale ENISA. (5) **Consiliul de administrație emite un aviz** cu privire la conturile finale ale ENISA pentru anul N. **Contabilul agenției întocmește conturile finale ale ENISA pe propria răspundere. Directorul executiv le prezintă consiliului de administrație în vederea obținerii unui aviz.**			
Articolul 52 Declarația de interese	Părțile **întocmesc declarație de angajamente și o declarație în care menționează absența sau prezența** oricăror interese directe sau indirecte despre care s-ar putea considera că aduc atingere independenței lor.	Conducerea ENISA (director executiv, director executiv adjunct); Consiliul de administrație, Experți naționali detașați	Prelucrarea și schimbul de date privind declarațiile de interese	Prelucrarea datelor Fluxul datelor
Articolul 58 Ofițerii de legătură	(1) **Fiecare stat membru desemnează cel puțin doi ofițeri de legătură** [din cadrul autorității lor naționale de securitate cibernetică] în calitate de experți naționali detașați la ENISA și care să	ENISA Statele membre	Desemnarea ofițerilor de legătură și schimbul de informații	Prelucrarea datelor Fluxul datelor

	lucreze la sediul său sau la biroul său local, în conformitate cu articolul 59 alineatul (2). Comisia poate desemna, de asemenea, un ofițer de legătură. (2) Ofițerii de legătură desemnați de statele lor membre au dreptul de a **solicita și de a primi toate informațiile relevante din partea statelor membre ale acestora**, astfel cum se prevede în prezentul regulament, respectând pe deplin dreptul intern sau practicile statelor lor membre, în special în ceea ce privește protecția datelor și normele privind confidențialitatea.			
Articolul 67 Gestionarea informațiilor clasificate	După **consultarea Comisiei**, ENISA adoptă norme de securitate care pun în aplicare principiile de securitate cuprinse în normele de securitate ale Comisiei pentru protecția informațiilor sensibile neclasificate și a IUEC, astfel cum sunt prevăzute în Deciziile (UE, Euratom) 2015/443 și (UE, Euratom) 2015/444. Normele de securitate ale ENISA includ **dispoziții privind schimbul, prelucrarea și stocarea unor astfel de informații.**	ENISA Consiliul de administrație Comisia	Gestionarea informațiilor clasificate	Prelucrarea datelor Fluxul datelor
Articolele 68, 69, 70 Cooperarea cu entitățile Uniunii și cu autoritățile naționale Cooperarea cu părțile interesate Cooperarea cu țările terțe	ENISA cooperează și face schimb de informații cu privire la aspecte legate de securitatea cibernetică cu entitățile relevante ale Uniunii și cu autoritățile de supraveghere a pieței și de supraveghere; părți interesate relevante: autorități competente din țări terțe sau organizații internaționale	ENISA Europol ECCC Comitetul european pentru protecția datelor Publicul larg Consiliul	Schimbul de informații	Fluxul datelor

Articolul 72 privind informarea și consultarea publicului cu privire la sistemele europene de certificare a securității cibernetice	(2) Comisia menține și actualizează periodic un site dedicat care oferă informații cu privire la următoarele aspecte: (a) Sistemele europene de certificare a securității cibernetice a căror dezvoltare este solicitată; (b) prioritățile strategice pentru armonizarea produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate sau a cerințelor de securitate din legislația Uniunii, inclusiv domeniile potențiale pentru care ar putea fi solicitat un sistem european de certificare a securității cibernetice. (3) Comisia pune la dispoziția publicului, pe site-ul menționat la alineatul (2) de la prezentul articol, informațiile transmise de ENISA referitoare la cererea sa de a pregăti o propunere de sistem, astfel cum se menționează la articolul 73 și decizia sa de a accepta, respinge sau întrerupe o propunere de sistem transmisă de ENISA în conformitate cu articolul 74 alineatul (7).	Comisia Europeană Publicul larg ENISA	Menținerea site-ului de informare Acest lucru mandatează Comisia să furnizeze informații pe un site accesibil publicului și să furnizeze în permanență activități conexe de gestionare a datelor.	Serviciul public digital Soluția digitală
Articolul 72 privind informarea și consultarea publicului cu privire la sistemele europene de certificare a securității cibernetice	În cursul pregătirii de către ENISA a unei propuneri de sistem în temeiul articolului 74, **Parlamentul European, Consiliul pot solicita Comisiei**, în calitatea sa de președinte al ECCG, și ENISA să prezinte trimestrial informații relevante cu privire la proiectul unei propuneri de sistem. **La cererea Parlamentului European sau a Consiliului, ENISA, de comun acord cu Comisia** și fără a aduce atingere articolului 54, poate pune **la dispoziția Parlamentului European și a Consiliului părțile relevante ale proiectului unei**	ENISA Consiliul UE Parlamentul European	Solicitarea și transmiterea de informații cu privire la un proiect de propunere de sistem elaborat de ENISA	Fluxuri de date

	propuneri de sistem, într-un mod adecvat nivelului de confidențialitate necesar și, după caz, în mod restrâns. **Parlamentul European, Consiliul pot invita Comisia și ENISA să discute** aspecte legate de punerea în aplicare a sistemelor europene de certificare a securității cibernetice pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura de securitate cibernetică a entităților.			
Articolul 73 Solicitarea unui sistem european de certificare a securității cibernetice Articolul 74 Pregătirea și adoptarea sistemelor europene de certificare a securității cibernetice **(vizată la articolul 17)**	**Articolul 73** **(1) Comisia poate solicita ENISA să pregătească o propunere de sistem european de certificare a securității cibernetice** pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura de securitate cibernetică a entităților. În cazuri justificate în mod corespunzător, ECCG poate sugera Comisiei să prezinte o solicitare menționată la alineatul (1). (4) Atunci când pregătește cererea menționată la alineatul (1), **Comisia** consultă în mod corespunzător ENISA și ECCG și ține seama de opiniile tuturor **părților interesate relevante** și ale altor entități ale Uniunii, inclusiv, după caz, de cele care sunt relevante în temeiul legislației Uniunii în care un sistem european de certificare a securității cibernetice oferă prezumția de conformitate. Articolul 74 (3) Atunci când pregătește propunerea de sistem, ENISA **cooperează îndeaproape cu ECCG**.	Comisia Europeană ENISA ECCG Părțile interesate specializate	Pregătirea unei solicitări și a unui sistem de certificare și consultarea aferentă a părților interesate	Prelucrarea datelor Fluxuri de date Serviciul public digital (vizată la articolul 17)

	ECCG oferă ENISA asistență și consiliere de specialitate în ceea ce privește pregătirea propunerii de sistem și, după caz, a specificației tehnice justificative. **ENISA solicită membrilor ECCG să furnizeze un aviz scris cu privire la propunerea de sistem.** (4) **ENISA consultă părțile interesate** în timp util, prin intermediul unui proces de consultare formal, deschis, transparent și favorabil incluziunii. **ENISA cooperează, de asemenea, cu autoritățile publice relevante din statele membre și cu entitățile relevante ale Uniunii pentru a obține consiliere de specialitate** din partea acestora în ceea ce privește pregătirea propunerii de sistem și, după caz, a specificației tehnice justificative. (6) **ENISA transmite Comisiei propunerea de sistem** în termen de cel mult 60 de zile de la data solicitării menționate la alineatul (5). (7) Atunci când primește propunerea de **sistem**, **Comisia evaluează** dacă sistemul corespunde cererii formulate în conformitate cu articolul 73. (8) În cazul în care Comisia returnează către ENISA o propunere de sistem în vederea revizuirii în conformitate cu alineatul (7) litera (b), alineatele (4), (5) și (7) de la prezentul articol se aplică în consecință.			

Articolul 75 Întreținerea unui sistem european de certificare a securității cibernetice	(2) În cooperare cu Comisia și cu sprijinul ECCG și al subgrupului său de întreținere relevant, ENISA asigură întreținerea sistemelor europene de certificare a securității cibernetice, inclusiv în vederea unei posibile revizuiri a acestor sisteme de către Comisie. ENISA cooperează și face schimb de informații cu entitățile și grupurile relevante ale Uniunii în ceea ce privește activitățile de întreținere. (5) ECCG poate emite un aviz cu privire la întreținerea sistemelor europene de certificare a securității cibernetice.	Comisia Europeană ENISA ECCG Organisme de evaluare a conformității	ENISA asigură întreținerea. Aceasta include reuniuni periodice în format hibrid sau online, colectarea de informații, analiza și schimbul (în legătură cu un sistem european de certificare a securității cibernetice)	Prelucrarea datelor Fluxul datelor
Articolul 76 Evaluarea, revizuirea și retragerea unui sistem european de certificare a securității cibernetice	(1) Cel puțin o dată la patru ani după intrarea în vigoare a unui sistem european de certificare a securității cibernetice, ENISA evaluează impactul și eficacitatea sistemului respectiv, în cooperare cu subgrupul de întreținere relevant al ECCG și ținând seama de feedbackul primit de la părțile interesate. ENISA efectuează evaluarea efectuând analiza de piață necesară în conformitate cu articolul 8 alineatul (1). (3) Atunci când revizuiește sau retrage sistemele europene de certificare a securității cibernetice, Comisia consultă ENISA, ECCG și subgrupul său de întreținere relevant și ține seama de opiniile părților interesate relevante și ale altor entități ale Uniunii. (4) ECCG poate emite un aviz cu privire la revizuirea sau retragerea unui sistem european de certificare a securității cibernetice. Comisia ține seama în mod corespunzător de acesta atunci când revizuiește sau retrage sistemul european de certificare a securității cibernetice.	Comisia Europeană ENISA ECCG	Comisia revizuiește sistemele consultând părțile interesate relevante.	Prelucrarea datelor Fluxul datelor

Articolul 77 Specificații tehnice în sistemele europene de certificare a securității cibernetice	(3) În cazul în care specificațiile tehnice sunt menționate într-un sistem european de certificare a securității cibernetice, astfel cum se menționează la articolul 74 alineatul (10), acestea sunt puse la dispoziție pe site-ul menționat la articolul 79. (4) În cazuri justificate în mod corespunzător, în special în cazul în care specificațiile tehnice conțin informații care ar putea compromite securitatea produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate certificate sau a posturii certificate de securitate cibernetică a entităților, acestea sunt distribuite numai părților interesate vizate de cerințele sistemului. Un astfel de sistem nu trebuie să fie menționat într-un sistem european de certificare a securității cibernetice, astfel cum se menționează la articolul 74 alineatul (10).	ENISA Statele membre Organisme de evaluare a conformității	Punerea la dispoziție a informațiilor pe site-ul ENISA dedicat certificării	Fluxul datelor Serviciul public digital
Articolul 79 Site-ul referitor la sistemele europene de certificare a securității cibernetice	(1) ENISA organizează activități de promovare a adoptării sistemelor europene de certificare a securității cibernetice adoptate, inclusiv prin menținerea site-ului menționat la alineatul (2) de la prezentul articol. (2) ENISA menține și actualizează periodic un site dedicat care oferă informații publice cu privire la următoarele: (a) sistemele europene de certificare a securității cibernetice; (b) taxele aferente întreținerii fiecărui sistem european de certificare a securității cibernetice; (c) specificațiile tehnice relevante ale ENISA; (d) certificatele europene de securitate cibernetică și declarațiile de conformitate UE,	ENISA Statele membre Organisme de evaluare a conformității	Menținerea site-ului de informare mandatează ENISA să colecteze, să prelucreze și să mențină baze de date cuprinzătoare cu informații de certificare, necesitând activități continue de gestionare a datelor.	Serviciul public digital Soluția digitală Prelucrarea datelor Fluxul datelor

	inclusiv informații cu privire la certificatele și declarațiile care nu mai sunt valabile sau care sunt suspendate, retrase sau expirate; (e) informațiile suplimentare relevante în materie de securitate cibernetică furnizate în conformitate cu articolul 84 alineatul (2); (f) rezumatele evaluărilor *inter pares* în temeiul articolului 89 alineatul (7); (g) specificațiile tehnice menționate într-un sistem european de certificare a securității cibernetice în temeiul articolului 74 alineatul (10). (3) După caz, **site-ul menționat la alineatul (2) indică și** sistemele naționale de certificare a securității cibernetice care au fost înlocuite de un sistem european de certificare a securității cibernetice.			
Articolul 81 Elemente ale sistemelor europene de certificare a securității cibernetice	(5) Comisia este împuternicită să adopte acte de punere în aplicare de stabilire a unor principii comune și a unor modele de dispoziții pentru elementele prevăzute la alineatele (1), (2) și (3) în cadrul sistemelor europene de certificare a securității cibernetice. Dacă este cazul și dacă este disponibil, un sistem european de certificare a securității cibernetice poate include trimiteri la aceste principii și modele de dispoziții. Actele de punere în aplicare prevăzute la alineatul (5) se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2). **Atunci când elaborează sau revizuiește principiile comune și modelele de dispoziții pentru elementele sistemelor europene de certificare a securității**	ENISA Publicul larg Autoritățile statelor membre	Consultarea părților interesate relevante care necesită fluxuri de date și prelucrare	Fluxul datelor Prelucrarea datelor

	cibernetice, Comisia consultă ENISA și ia în considerare, după caz, opiniile exprimate de ECCG, de părțile interesate relevante și de alte organisme relevante.			
Articolul 83 Autoevaluarea conformității	(3) Producătorul sau furnizorul de produse TIC, servicii TIC, procese TIC, servicii de securitate gestionate sau entitatea a cărei postură de securitate cibernetică face obiectul certificării pune declarația de conformitate UE, documentația tehnică și toate celelalte informații relevante referitoare la conformitatea produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate sau a posturii de securitate cibernetică cu sistemul european de certificare a securității cibernetice la dispoziția autorității naționale de certificare a securității cibernetice desemnate în temeiul articolului 89 pentru perioada prevăzută în sistemul respectiv. **O copie a declarației de conformitate UE se transmite fără întârzieri nejustificate către autoritatea națională de certificare a securității cibernetice și către ENISA.**	ENISA Publicul larg Autoritățile statelor membre	Disponibilitatea informațiilor; partajare de date Datele partajate necesită prelucrarea de către ENISA și autoritățile statelor membre	Fluxul datelor Prelucrarea datelor
Articolul 84 Informații suplimentare privind securitatea cibernetică pentru produsele TIC, serviciile TIC și procesele TIC certificate	(1) Producătorul sau furnizorul de produse TIC, servicii TIC sau procese TIC pentru care a fost eliberată o declarație de conformitate UE sau un certificat european de securitate cibernetică **trebuie să pună la dispoziția publicului următoarele informații suplimentare în materie de securitate cibernetică**.	Producător sau furnizor de produse TIC, de servicii TIC sau de procese TIC Publicul larg Organisme de evaluare a conformității	Punerea informațiilor la dispoziția publicului în format electronic.	Fluxul datelor
Articolul 85 Eliberarea certificatelor europene de securitate	(2) Organismele de evaluare a conformității menționate la articolul 91 eliberează certificate europene de securitate cibernetică pe baza	ENISA Publicul larg Autoritățile statelor membre	Schimbul de informații relevante pentru procesele de certificare	Fluxul datelor Prelucrarea datelor

cibernetică	criteriilor incluse în sistemul european de certificare a securității cibernetice adoptat în temeiul articolului 74. (6) Persoana fizică sau juridică care supune certificării produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate sau entitatea care solicită certificarea posturii sale de securitate cibernetică **trebuie să pună la dispoziția autorității naționale de certificare a securității cibernetice desemnate în temeiul articolului 89, în cazul în care autoritatea respectivă este organismul care eliberează certificatul european de securitate cibernetică, sau a organismului de evaluare a conformității menționat la articolul 91, toate informațiile necesare pentru efectuarea certificării**. (7) Organismele de evaluare a conformității și, după caz, **autoritățile naționale de certificare a securității cibernetice informează ENISA** fără întârzieri nejustificate cu privire la deciziile lor care afectează statutul certificatelor europene de securitate cibernetică și al declarațiilor de conformitate UE în conformitate cu articolul 94. (8) **Deținătorul unui certificat european de securitate cibernetică informează organismul de evaluare a conformității** și, după caz, autoritatea națională de certificare a securității cibernetice, menționate la alineatul (7), cu privire la orice vulnerabilități sau neconformități detectate ulterior în ceea ce privește produsul TIC, serviciul TIC, procesul TIC, serviciul de securitate gestionat sau postura de securitate cibernetică certificată a entității care au un	Organisme de evaluare a conformității		

	impact probabil asupra conformității sale cu certificatul. **Organismul respectiv transmite informațiile respective fără întârzieri nejustificate** autorității naționale de certificare a securității cibernetice în cauză și evaluează impactul asupra certificatului în conformitate cu condițiile sistemului menționate la articolul 81 litera (f).			
Articolul 86 Sistemele naționale de certificare a securității cibernetice	(4) **Statele membre informează Comisia și ECCG înainte de a adopta noi sisteme naționale de certificare a securității cibernetice** pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate și postura de securitate cibernetică a entităților.	ENISA statele membre Comisia Europeană	Schimb de informații	Fluxul datelor
Articolul 88 Autoritățile naționale de certificare a securității cibernetice	(2) Fiecare stat membru **informează Comisia cu privire la identitatea autorităților naționale de certificare a securității cibernetice desemnate**. În cazul în care un stat membru desemnează mai multe autorități, acesta informează Comisia și cu privire la sarcinile atribuite fiecăreia dintre respectivele autorități. (6) Autoritățile naționale de certificare a securității cibernetice: (c) **monitorizează, în cooperare cu autoritățile relevante de supraveghere a pieței, respectarea și asigurarea respectării obligațiilor producătorilor sau furnizorilor** de produse TIC, servicii TIC, procese TIC, servicii de securitate gestionate sau ale entităților a căror postură de securitate cibernetică este certificată, prevăzute în prezentul regulament, care sunt stabiliți pe teritoriile lor respective și care	ENISA Autoritățile statelor membre Comisia Europeană Publicul larg Organisme de evaluare a conformității	Statul membru informează Comisia cu privire la ANCSC-urile desemnate Autoritățile statelor membre îndeplinesc diverse sarcini de monitorizare, supraveghere și cooperare care necesită fluxuri de date și prelucrarea datelor.	Fluxul datelor Prelucrarea datelor

	efectuează autoevaluarea conformității și în sistemul european de certificare a securității cibernetice; corespunzător; (d) fără a aduce atingere articolului 91 alineatul (3), **asistă și sprijină activ organismele naționale de acreditare sau alte autorități relevante la monitorizarea și supravegherea** activităților organismelor de evaluare a conformității în sensul prezentului regulament; (e) cooperează cu Comisia Europeană în cazul în care competența unui organism de evaluare a conformității este contestată în temeiul articolului 94; (f) **monitorizează și supraveghează activitățile** organismelor publice menționate la articolul 85 alineatul (3); (g) după caz, autorizează organismele de evaluare a conformității în conformitate cu articolul 93, monitorizează respectarea obligațiilor organismelor de evaluare a conformității și asigură respectarea de către acestea a cerințelor specifice sau suplimentare prevăzute în sistemele europene de certificare a securității cibernetice în temeiul articolului 81 alineatul (3) litera (f) și restricționează, suspendă sau retrage autorizația existentă în cazul în care organismele de evaluare a conformității nu îndeplinesc cerințele prezentului regulament; (h) **gestionează plângerile** persoanelor fizice sau juridice în legătură cu certificatele europene de securitate cibernetică eliberate de autoritățile naționale de certificare a securității			

	cibernetice sau cu cele eliberate de organismele de evaluare a conformității în conformitate cu articolul 85 alineatul (4), sau în legătură cu declarațiile de conformitate UE eliberate în temeiul articolului 83, investighează, în măsura în care este oportun, subiectul plângerii și informează reclamantul despre stadiul și rezultatul investigației, într-un termen rezonabil; (i) prezintă Comisiei, ENISA și ECCG un raport anual cu privire la principalele sale activități până la data de 31 martie a fiecărui an, începând din [anul intrării în vigoare + 12 luni] și pune aceste rapoarte la dispoziția echipei de evaluare *inter pares* în cazul în care autoritatea națională de certificare a securității cibernetice face obiectul unei evaluări *inter pares* în conformitate cu articolul 89; (j) **cooperează cu alte autorități naționale de certificare a securității cibernetice**, autorități de supraveghere a pieței sau cu alte autorități publice, inclusiv prin schimbul de informații cu privire la o posibilă neconformitate a produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate și a posturii de securitate cibernetică a entităților cu cerințele prezentului regulament sau cu cerințele sistemului european de certificare a securității cibernetice specific; (k) **monitorizează evoluțiile relevante din domeniul certificării securității cibernetice**. (8) Autoritățile naționale de certificare a securității cibernetice cooperează între ele și cu Comisia, în special prin **schimb de**			

	informații, de experiență și de bune practici în ceea ce privește certificarea securității cibernetice și aspectele tehnice privind securitatea cibernetică a produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate și a posturii cibernetice a entităților. (9) Până la [data intrării în vigoare + 6 luni], ENISA elaborează un model pentru raportul menționat la alineatul (6) litera (i) de la prezentul articol, în cooperare cu Comisia și cu ECCG.			
Articolul 89 Evaluarea *inter pares*	(5) **ENISA sprijină** organizarea mecanismului de evaluare *inter pares* și a evaluărilor *inter pares*, inclusiv **prin elaborarea de documente de orientare și modele relevante**, în cooperare cu Comisia și cu ECCG. (7) **Raportul final, inclusiv posibilele** orientări sau recomandări, rezumatul evaluării *inter pares* sunt examinate de ECCG, care aprobă rezumatul în vederea publicării pe site-ul menționat la articolul 79 alineatul (2).	UE ENISA ECCG	Punerea la dispoziție online a datelor	Fluxul datelor Prelucrarea datelor
Articolul 90 Grupul european de certificare a securității cibernetice (ECCG)	(3) ECCG are următoarele atribuții: [trimitere la alte articole] (h) să examineze evoluțiile relevante în domeniul certificării de securitate cibernetică, inclusiv la nivel național în temeiul articolului 86, și să facă schimb de informații și de bune practici cu privire la sistemele de certificare a securității cibernetice; (i) să faciliteze cooperarea dintre autoritățile naționale de certificare a securității cibernetice în temeiul normelor	statele membre ENISA Comisia Europeană	Analiza, schimbul de informații și cooperarea dintre autoritățile statelor membre și organizațiile internaționale în ceea ce privește certificarea europeană de securitate cibernetică	Prelucrarea datelor Fluxul datelor

	prevăzute în prezentul titlu prin consolidarea capacităților și schimbul de informații, în special în ceea ce privește aspectele legate de certificarea securității cibernetice; [trimitere la alte articole] (k) să faciliteze alinierea sistemelor europene de certificare a securității cibernetice la standardele recunoscute la nivel internațional, inclusiv ca parte a întreținerii sistemelor europene de certificare a securității cibernetice existente și, după caz, să facă recomandări ENISA pentru a colabora cu organizațiile de standardizare europene sau internaționale relevante pentru a remedia insuficiențele sau lacunele standardelor europene sau recunoscute la nivel internațional disponibile.			
Articolul 92 Armonizarea suplimentară a competenței organismelor de evaluare a conformității	(4) În cazul în care o autoritate națională de certificare a securității cibernetice primește o cerere în temeiul alineatului (3), aceasta **informează autoritatea națională de certificare a securității cibernetice a statului membru în care este stabilit organismul de evaluare a conformității solicitant**. În aceste cazuri, autoritatea națională de certificare a securității cibernetice din statul membru respectiv poate participa la autorizare în calitate de observator.	Autoritățile statelor membre Organisme de evaluare a conformității	Schimbul de informații și păstrarea acestora	Fluxul datelor Prelucrarea datelor
Articolul 93 Notificarea organismelor de evaluare a conformității	(1) Pentru fiecare sistem european de certificare a securității cibernetice, **autoritățile naționale de certificare a securității cibernetice ale unui stat membru notifică Comisiei și celorlalte state membre** organismele de evaluare a conformității care au fost acreditate și, după caz,	ENISA Statele membre Comisia Europeană Organisme de evaluare a conformității	Notificările organismelor acreditate și autorizate de evaluare a conformității	Fluxuri de date Prelucrarea datelor

	autorizate în temeiul articolului 92. (2) **Autoritățile naționale de certificare a securității cibernetice efectuează notificarea menționată la alineatul (1)** utilizând instrumentul de notificare electronică dezvoltat și gestionat de Comisie.			
Articolul 94 Contestarea competenței organismelor de evaluare a conformității	1. (1) **Comisia investighează** toate cazurile în care are îndoieli sau i se aduc la cunoștință îndoieli cu privire la competența unui organism de evaluare a conformității de a îndeplini cerințele și responsabilitățile care îi revin sau la continuarea îndeplinirii acestora de către un organism de evaluare a conformității. (2) **Autoritatea națională de certificare a securității cibernetice prezintă Comisiei,** la cerere, toate informațiile referitoare la temeiul notificării sau la menținerea competenței organismului de evaluare a conformității în cauză. (3) **Comisia se asigură că toate informațiile sensibile obținute pe parcursul investigațiilor sale sunt tratate în mod confidențial.** (4) În cazul în care constată că un organism de evaluare a conformității nu îndeplinește sau nu mai îndeplinește cerințele pentru a fi notificat, Comisia **informează autoritatea națională de certificare a securității cibernetice în consecință** și solicită acesteia să ia măsurile corective necesare, inclusiv anularea notificării, dacă este necesar.	Comisia Statele membre ENISA	Contestarea competenței organismelor de evaluare a conformității	Fluxul datelor Prelucrarea datelor Serviciul public digital
Articolul 95 Obligația de informare și de păstrare a informațiilor impusă	(1) Organismele de evaluare a conformității **informează autoritatea națională de certificare a securității cibernetice** cu privire	Autoritățile statelor membre Organisme de evaluare a conformității	Schimbul de informații de la organismele de evaluare a conformității	Fluxul datelor Prelucrarea datelor

organismelor de evaluare a conformității	la următoarele: (a) orice refuzare, restricționare, suspendare sau retragere a unui certificat; (b) orice circumstanțe care afectează domeniul de aplicare și condițiile notificării menționate la articolul 93 alineatul (1); (c) orice cerere de informare cu privire la activitățile de evaluare a conformității, primită de la autoritățile de supraveghere a pieței; (d) la cerere, orice activitate de evaluare a conformității desfășurată în sfera notificării sale și orice alte activități desfășurate, inclusiv activități transfrontaliere și subcontractarea. (2) **Organismele de evaluare a conformității furnizează, de asemenea, ENISA informațiile** menționate la alineatul (1) litera (a) pentru a facilita îndeplinirea sarcinilor care îi revin în temeiul articolului 79. (3) **Organismele de evaluare a conformității furnizează celorlalte organisme de evaluare a conformității** în temeiul prezentului regulament care desfășoară activități similare de evaluare a conformității și care vizează aceleași produse TIC, servicii TIC, procese TIC, servicii de securitate gestionate sau entități a căror postură de securitate cibernetică este certificată, fără întârzieri nejustificate, **informații relevante** privind aspecte legate de rezultate negative și, la cerere, pozitive			

	ale evaluării conformității. (4) **Organismele de evaluare a conformității țin un sistem de evidență** care conține toate documentele și dovezile prezentate sau primite în legătură cu fiecare evaluare și certificare pe care o efectuează. Evidențele se stochează într-un mod securizat și accesibil pe perioada necesară în scopul certificării și timp de cel puțin cinci ani de la expirarea sau retragerea unui certificat european de securitate cibernetică relevant.			
Articolul 96 Dreptul de a depune o plângere și dreptul la o cale de atac eficientă	(2) Autoritatea sau organismul la care s-a depus plângerea **informează reclamantul despre evoluția** procedurilor, despre decizia luată și despre dreptul de a exercita o cale de atac eficientă în temeiul alineatelor (3) și (4). (4) Acțiunile în temeiul prezentului articol se introduc în fața instanțelor din statul membru în care este situată autoritatea sau organismul împotriva căruia se exercită calea de atac.	Autoritățile statelor membre Comisia Europeană Publicul larg Deținătorii de certificate	Fluxul de informații între autorități și publicul larg cu privire la plângeri Proceduri în fața instanțelor din statul membru	Fluxul datelor
Articolul 97 Sancțiuni	**Statele membre informează Comisia fără întârziere** cu privire la normele și măsurile respective și notifică acesteia orice modificare ulterioară care le afectează.	Autoritățile statelor membre Comisia Europeană	Fluxul de informații privind notificarea Comisiei de către statele membre cu privire la sancțiuni.	Fluxul datelor

Articolul 99 Evaluările riscurilor în materie de securitate	Comisia sau cel puțin trei state membre pot solicita GC NIS să efectueze evaluări coordonate ale riscurilor în termen de șase luni. Comisia poate solicita termene mai scurte. Evaluările riscurilor elaborează scenarii de risc și presupun analiza datelor. Elaborarea evaluărilor coordonate ale riscurilor în materie de securitate În cazurile care justifică o intervenție imediată, Comisia consultă fără întârziere statele membre și efectuează o evaluare a riscurilor. Decizii pentru efectuarea de evaluări ale riscurilor (prelucrarea/analiza datelor).	Comisia Europeană State membre ale UE Grupul de cooperare NIS ENISA	Solicitarea și primirea de informații; analiza datelor în scopul evaluărilor coordonate ale riscurilor Consultarea cu statele membre și efectuarea unei evaluări a riscurilor	Prelucrarea datelor Fluxul datelor
Articolul 100 alineatele (1) și (2) Desemnarea țărilor terțe care prezintă motive de îngrijorare în materie de securitate cibernetică	(1) În cazul în care, ca urmare a evaluării riscurilor în materie de securitate menționate la articolul 99 sau pe baza altor surse, cum ar fi o declarație publică în numele Uniunii sau al unui stat membru, reiese că o țară terță prezintă riscuri non-tehnice grave și structurale la nivelul lanțurilor de aprovizionare TIC, Comisia verifică amenințarea reprezentată de țara respectivă, ținând seama de o serie elemente, conducând la prelucrarea/analiza datelor. (2) În cazul în care, în urma verificării menționate la alineatul (1), Comisia concluzionează că o țară terță prezintă riscuri non-tehnice grave și structurale la	State membre ale UE Comisia Europeană	Primirea de informații, analizarea informațiilor, schimbul de informații.	Fluxuri de date Prelucrarea datelor

	nivelul lanțurilor de aprovizionare TIC, aceasta poate decide, prin intermediul unui act de punere în aplicare, să desemneze țara terță respectivă ca țară care prezintă motive de îngrijorare în materie de securitate cibernetică a lanțurilor de aprovizionare TIC, conducând la prelucrarea datelor, analiză și fluxuri de date.			
Articolul 101 Mecanismul general al lanțului de aprovizionare TIC Articolul 102 Identificarea activelor TIC esențiale și Articolul 103 Măsuri de atenuare în cadrul lanțurilor de aprovizionare	(1) În cazul în care Grupul de cooperare NIS a efectuat o evaluare coordonată la nivelul Uniunii a riscurilor în materie de securitate în temeiul articolului 99 alineatele (1) și (2) din prezentul regulament sau după finalizarea procedurii în cazul unei amenințări cibernetice semnificative în temeiul articolului 99 alineatul (3), Comisia poate lua măsurile prevăzute la articolele 102 și 103. Comisia este împuternicită să adopte acte de punere în aplicare, care vor defini activele TIC esențiale și măsuri de atenuare, inclusiv restricții și interdicții privind lanțurile de aprovizionare TIC (detaliate în secțiunea 4.5 de mai jos). În pregătirea acestui proces, Comisia ține seama și ia în considerare mai multe aspecte care evocă **prelucrarea/analizarea datelor și, în unele cazuri, fluxul de date**:	Comisia Europeană Grupul de cooperare NIS Părți interesate relevante	Analiza datelor/prelucrarea datelor; consultarea părților interesate relevante	Prelucrarea datelor Fluxul datelor

TIC	Articolul 102 literele (a)-(f) Articolul 103 alineatul (4) literele (a)-(d) Articolul 103 alineatul (6)			
Articolul 104 Identificarea furnizorilor cu grad ridicat de risc	Prin intermediul unor acte de punere în aplicare, Comisia stabilește liste cu furnizorii cu grad ridicat de risc relevanți pentru interdicțiile prevăzute în actele de punere în aplicare adoptate în conformitate cu articolul 103 alineatul (1) sau pentru interdicția menționată la articolul 111 alineatul (1). Comisia cartografiază furnizorii care furnizează componente TIC și componente care includ componente TIC și efectuează o evaluare inițială, cu privire la furnizorii care ar putea fi stabiliți sau controlați din țări terțe desemnate în conformitate cu articolul 100. Comisia evaluează locul de stabilire, precum și structura de proprietate și de control. Comisia are dreptul de a solicita informațiile necesare de la furnizori, de a comunica constatările preliminare privind evaluarea stabilirii, a proprietății și controlului furnizorului în cauză și de a-i acorda	Comisia Europeană Autoritățile competente Furnizori	Analiza datelor/prelucrarea datelor; consultarea cu autoritățile competente, consultarea cu furnizorii	Prelucrarea datelor Fluxul datelor

	acestuia posibilitatea de a fi audiat. Comisia poate solicita unei autorități competente să efectueze evaluarea inițială privind stabilirea, proprietatea și controlul unui furnizor, în cazul în care acest lucru este justificat având în vedere caracteristicile activității furnizorului respectiv. O autoritate competentă se poate oferi să efectueze o astfel de evaluare inițială. Comisia verifică aceste constatări inițiale pentru a decide dacă furnizorul ar trebui inclus pe lista furnizorilor cu grad ridicat de risc. Comisia actualizează periodic listele furnizorilor cu grad ridicat de risc în vederea eliminării sau a adăugării de furnizori cu grad ridicat de risc. Furnizorii cu grad ridicat de risc incluși pe listă pot solicita Comisiei să reevalueze înființarea, controlul și structura de proprietate a acestora, pe baza furnizării de dovezi că au existat modificări relevante.			
Articolul 105 Derogare pentru entitățile stabilite într-o țară terță sau controlate de entități dintr-o țară terță care prezintă motive de îngrijorare în materie de securitate cibernetică	(1) O entitate stabilită într-o țară terță sau controlată de o țară terță care prezintă motive de îngrijorare în materie de securitate cibernetică **poate adresa Comisiei o cerere motivată**. (3) Comisia evaluează și adoptă o decizie **ținând seama de mai multe aspecte** care	Comisia Europeană Entități stabilite într-o țară terță sau controlate de entități dintr-o țară terță desemnată care prezintă motive de îngrijorare în materie de securitate cibernetică	Primirea cererii de către Comisie; analiza datelor.	Fluxul datelor Prelucrarea datelor

Articolul 108 Confidențialitate	conduc la analiza datelor. [articolul 105 alineatele (3) și (4)] Informațiile primite de Comisie se utilizează numai în scopul pentru care au fost obținute.			
Articolul 107 Registrul	Comisia ține un registru accesibil publicului cu deciziile sale menționate la articolul 105. Registrul menționează numele entităților care au făcut obiectul deciziilor.	Comisia Europeană Entități stabilite într-o țară terță sau controlate de o țară terță desemnată care prezintă motive de îngrijorare în materie de securitate cibernetică	Comisia ține un registru accesibil publicului.	Soluția digitală
Articolul 111 Interdicții privind rețelele de comunicații electronice mobile, fixe și prin satelit	Autoritatea competentă desemnată în temeiul prezentului regulament **informează** fără întârziere autoritatea competentă în temeiul Regulamentului (UE) XX/XXXX [propunerea DNA] cu privire la măsurile impuse furnizorilor de rețele de comunicații electronice mobile, fixe și prin satelit.	Autoritate competentă în sensul articolului 9 sau 20 din Regulamentul (UE) XX/XXXX [propunerea DNA] Furnizori de rețele de comunicații electronice mobile, fixe și prin satelit	Fluxul de informații de la autoritatea competentă către entități în legătură cu autorizațiile.	Fluxul datelor
Articolul 112 alineatele (1), (4) Autoritățile competente	(1) **Fiecare stat membru desemnează** una sau mai multe autorități competente responsabile cu sarcinile de supraveghere și de asigurare a respectării legislației menționate la articolul 114. (4) Fiecare stat membru notifică Comisiei, fără întârzieri nejustificate, numele	State membre ale UE Comisia Europeană Publicul larg	Desemnarea de către statele membre a autorităților competente și notificarea Comisiei.	Fluxul datelor

	autorităților competente desemnate în conformitate cu alineatul (1), sarcinile respective ale acestor autorități și orice modificări ulterioare ale acestora. De asemenea, fiecare stat membru face publice denumirile autorităților competente desemnate în conformitate cu alineatul (1).			
Articolul 113 Rețeaua pentru cooperare și servicii de sprijin a Comisiei	(1) Comisia instituie o rețea de cooperare a autorităților competente ale statelor membre și a Comisiei, care să servească drept platformă pentru cooperare și schimb de informații. Comisia oferă sprijin administrativ rețelei. (2) Pentru a sprijini statele membre în îndeplinirea sarcinilor lor de supraveghere, Comisia evaluează dacă furnizorii care pot fi afectați de interdicții specifice sunt stabiliți în țări terțe care prezintă motive de îngrijorare în materie de securitate cibernetică, desemnate în temeiul articolului 100 sau controlați din acestea. În acest scop, autoritatea competentă face schimb de informații relevante cu Comisia. (3) În scopul evaluării, Comisia are dreptul de a solicita informațiile necesare de la furnizorii care pot fi afectați de interdicții specifice care sunt stabiliți în țări terțe desemnate în temeiul articolului 100 sau	Comisia Autoritățile competente Entitățile de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555	Evaluarea de către Comisie a furnizorilor și partajarea cu autoritățile competente care partajează cu entități de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555 Comisia solicită informații de la furnizori Informarea Comisiei de către autoritățile competente	Prelucrarea datelor Fluxuri de date

	sunt controlați din astfel de țări. (4) După finalizarea unei evaluări, Comisia transmite constatările autorităților competente din cadrul rețelei instituite în temeiul alineatului (1). Autoritățile competente informează în timp util entitățile în cauză de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555 cu privire la constatări. (5) În cazul în care o autoritate competentă ia cunoștință de faptul că un furnizor care poate fi afectat de interdicții specifice este stabilit în țări terțe sau controlat din țări terțe care ridică motive de îngrijorare privind securitatea cibernetică și care nu a fost supus unei evaluări, aceasta informează Comisia fără întârzieri nejustificate.			
Articolul 114 Măsuri de supraveghere și de asigurare a respectării legislației	Cerințe pentru statele membre care vor asigura fluxul de informații cu entitățile menționate în anexele I și II la Directiva (UE) 2022/2555. Înainte de a adopta de măsuri, autoritățile competente notifică entităților în cauză constatările lor preliminare. Autoritățile competente cooperează între ele și cu Comisia.	State membre ale UE Comisia Europeană Entități în contextul anexelor I și II la Directiva (UE) 2022/2555	Cerințe care să asigure fluxul de informații;	Fluxul datelor Prelucrarea datelor

Articolul 115 Sancțiuni	Statele membre notifică normele respective Comisiei și îi comunică acesteia, fără întârziere, orice modificări ulterioare privind aceste norme.	Comisia Europeană State membre ale UE	Notificarea Comisiei de către statele membre	Fluxul datelor
Articolul 116 Asistența reciprocă	Dacă o entitate menționată în anexa I sau II din Directiva (UE) 2022/2555 furnizează servicii în mai multe state membre sau furnizează servicii în unul sau mai multe state membre iar activele sale esențiale sunt situate în unul sau mai multe alte state membre, **autoritățile competente ale statelor membre în cauză cooperează și își oferă asistență reciprocă, după caz**. Asistența reciprocă menționată la primul paragraf litera (c) poate acoperi cererile de informații și măsurile de supraveghere, inclusiv cererile de efectuare a unor inspecții la fața locului, a unei supravegheri *ex situ* sau a unor audituri de securitate specifice. O autoritate competentă căreia i se adresează o cerere de asistență nu refuză cererea respectivă, cu excepția cazului în care se stabilește că nu are competența de a furniza asistența solicitată, asistența solicitată nu este proporțională cu sarcinile de supraveghere ale autorității competente sau cererea privește informații sau implică	State membre ale UE	Asistență reciprocă în ceea ce privește acțiunile de supraveghere.	Fluxul datelor Prelucrarea datelor

	activități care, dacă ar fi divulgate sau desfășurate, ar fi contrare intereselor esențiale ale statului membru respectiv în materie de securitate națională, siguranță publică sau apărare. Înainte de a refuza o astfel de cerere, autoritatea competentă consultă celelalte autorități competente în cauză, precum și, la cererea unuia dintre statele membre în cauză, Comisia. Dacă este cazul și de comun acord, autorități competente din diferite state membre pot desfășura acțiuni comune de supraveghere.			
Articolul 1 punctul 8 din directivă Raportarea atacurilor de tip ransomware [Articolul 27 alineatul (13) din NIS2]	La articolul 23, se adaugă următoarele alineate (12) și (13): „(13) Statele membre se asigură că, în cazul unui incident semnificativ cauzat de un atac de tip ransomware, entitățile în cauză informează, la cererea echipei CSIRT sau, după caz, a autorității competente, prin intermediul unui canal de comunicare furnizat de echipa CSIRT sau, după caz, de autoritatea competentă: dacă entitatea a primit o cerere de răscumpărare și, după caz, de la cine; dacă s-a plătit o răscumpărare și, în caz afirmativ, ce sumă a fost plătită și cărui destinatar sau beneficiar, inclusiv criptoactivul și prestatorul de servicii de criptoactive, după caz.”	State membre ale UE Entități esențiale și entități importante	Raportare	Fluxul datelor

Articolul 1 punctul 10 din directivă Lista entităților și registrul [Articolul 27 alineatul (1) din NIS2]	**ENISA creează și menține un registru al entităților esențiale și al entităților importante, precum și al entităților care furnizează servicii de înregistrare a numelor de domenii, pe baza informațiilor primite de la punctele unice de contact în conformitate cu alineatul (2)**.	ENISA Statele membre ale UE (entități esențiale și entități importante în temeiul NIS2, entități care furnizează servicii de înregistrare a numelor de domenii)	ENISA creează și menține un registru.	Soluția digitală Serviciul public digital
Articolul 1 punctul 11 din directivă Lista entităților și registrul [Articolul 27 alineatul (4) din NIS2]	**„(4) La primirea informațiilor menționate la articolul 3 alineatul (4), punctul unic de contact al statului membru în cauză le transmite către ENISA fără întârzieri nejustificate.”**	ENISA State membre ale UE	Schimbul de informații între statele membre și ENISA	Fluxul datelor
Articolul 1 punctul 12 din directivă Asistența reciprocă [Articolul 37a alineatele (1), (2), (3) din NIS2]	**(1) ENISA asistă statele membre** în furnizarea de asistență reciprocă în sensul articolului 37 și **contribuie la facilitarea unor astfel de procese de cooperare** pentru entitățile esențiale și entitățile importante (...). (2) ENISA **efectuează o analiză cuprinzătoare** (...) **ENISA elaborează o metodologie în cooperare cu** Comisia și cu grupul de cooperare. Raportul se actualizează anual. (3) După caz, ENISA face recomandări; elaborează de orientări; oferă asistență (...)	ENISA State membre ale UE Entități importante și entități esențiale în sensul Directivei NIS2 Comisia Europeană	ENISA asistă statele membre și contribuie la facilitarea procesului de cooperare. Efectuarea de analize, orientări, metodologie, rapoarte.	Prelucrarea datelor Fluxul datelor
Articolul 1 punctul 12 din directivă Asistența reciprocă [Articolul 37a alineatul (4) din NIS2]	(4) În sensul alineatului (4) litera (e) de la prezentul articol, autoritățile competente ale **statelor membre în cauză transmit ENISA**, dacă sunt disponibile, următoarele informații (...). (5) În cazul în care un stat membru primește asistență reciprocă, astfel cum se menționează la	ENISA State membre ale UE	Schimbul de informații	Fluxul datelor

	articolul 37 alineatul (1) primul paragraf litera (c), **punctul unic de contact informează ENISA** că a avut loc asistența reciprocă.			
Articolul 119 Exercitarea delegării de competențe	(3) De îndată ce adoptă un act delegat, Comisia **îl notifică simultan** Parlamentului European și Consiliului.	Comisia Europeană Parlamentul European Consiliul	Informații transmise PE și Consiliului	Fluxul datelor
Articolul 120 Evaluare și revizuire	(1) Până la [ZZ LL AAAA] și, ulterior, o dată la cinci ani, Comisia comandă o evaluare a performanței ENISA în raport cu obiectivele, mandatul, misiunea, sarcinile, guvernanța și localizarea acesteia, în conformitate cu orientările Comisiei. (5) Comisia prezintă Parlamentului European, Consiliului și consiliului de administrație un raport privind concluziile evaluării. Rezultatele evaluării se fac publice.	ENISA Comisia Publicul larg	Colectarea și analiza datelor; punerea informațiilor la dispoziția publicului	Prelucrarea datelor Fluxul datelor

4.2. Date

Descriere detaliată a datelor în ceea ce privește domeniul de aplicare și orice standarde/specificații aferente

Tipul de date	**Trimitere (trimiteri) la cerință**	**Standard și/sau specificație (dacă este cazul)**
Date legate de analize/rapoarte relevante pentru reziliența în materie	**Articolul 5 alineatul (1) litera (a), (b), (c), (e), (f), (h)**	În desfășurarea activităților enumerate la articolul 11 alineatul (1) literele (a)-(e) și la alineatul (2), ENISA utilizează propriile analize și, după caz, informațiile primite în îndeplinirea sarcinilor

de securitate cibernetică și societate	**Articolul 5 alineatele (2), (3) și (4)** **Articolul 6** **Articolul 7** **Articolul 8** **Articolul 9** **Articolul 10** **Articolul 11 alineatul (2) literele (b), (c)** **Articolul 12 alineatul (4)** **Articolul 15** **Articolul 1 punctul 7 din directivă**	sale, inclusiv: (a) informațiile furnizate din surse aflate la dispoziția publicului, inclusiv vulnerabilitățile cunoscute public ale produselor TIC sau ale serviciilor TIC disponibile în baza de date europeană a vulnerabilităților instituită în temeiul articolului 12 alineatul (2) din Directiva (UE) 2022/2555; (b) informațiile partajate de statele membre, entitățile Uniunii, CERT-UE, partenerii din sectorul privat sau neguvernamental și organizațiile din țări terțe și internaționale, sub rezerva oricăror limitări prin intermediul unui marcaj vizibil privind distribuirea ulterioară a informațiilor respective. ENISA emite orientări privind interoperabilitatea rețelelor și a sistemelor informatice utilizate pentru schimbul de informații, inclusiv în ceea ce privește centrele cibernetice transfrontaliere, astfel cum se menționează la articolul 6 alineatul (3) din Regulamentul (UE) 2025/38.
Date relevante pentru cooperarea operațională și conștientizarea situației	**Articolul 10 alineatul (4) literele (a)-(g)** **Articolul 10 alineatul (6)** **Articolul 11 alineatul (1) literele (a)-(g)** **Articolul 11 alineatul (2) literele (a), (b), (c)** **Articolul 11 alineatul (3)** **Articolul 11 alineatul (4)** **Articolul 13 alineatul (2)**	**Standarde de confidențialitate și de gestionare a informațiilor sensibile** În desfășurarea activităților enumerate la articolul 11 alineatul (1) literele (a)-(e) și la alineatul (2), ENISA utilizează propriile analize și, după caz, informațiile primite în îndeplinirea sarcinilor sale, inclusiv: (a) informațiile furnizate din surse aflate la dispoziția publicului, inclusiv vulnerabilitățile cunoscute public ale produselor TIC sau ale serviciilor TIC disponibile în baza de date europeană a vulnerabilităților instituită în temeiul articolului 12 alineatul (2) din Directiva (UE) 2022/2555; (b) informațiile partajate de statele membre, entitățile Uniunii, CERT-UE, partenerii din sectorul privat sau neguvernamental și organizațiile din țări terțe și internaționale, sub rezerva oricăror

	Articolul 15 **Articolul 16 alineatul (2) litera (e)**	limitări prin intermediul unui marcaj vizibil privind distribuirea ulterioară a informațiilor respective.
Date relevante pentru sistemele europene de atestare individuală a competențelor în materie de securitate cibernetică și pentru autorizarea furnizorilor **Date relevante pentru obiectivele, scopul și conținutul sistemelor europene de certificare a securității cibernetice**	**Articolul 17** **Articolul 18** **Articolele 19-23** **Articolele 72, 73, 74, 75, 76, 77, 79, 81, 83, 84**	Un sistem european de atestare individuală a competențelor în materie de securitate cibernetică trebuie să includă (...): norme privind păstrarea evidențelor de către furnizorii de atestate autorizați; Furnizorii autorizați se asigură că, la cererea persoanei, atestatele electronice aferente atestatelor europene individuale de competențe în materie de securitate cibernetică sunt emise ca atestate electronice ale atributelor într-un format care poate fi stocat în portofelele europene pentru identitatea digitală prevăzute în Regulamentul (UE) nr. 910/2014. . Comisia și ENISA ar trebui să respecte dispozițiile relevante ale legislației Uniunii atunci când instituie un sistem european de certificare a securității cibernetice în ceea ce privește datele.
Date referitoare la guvernanța cadrului european de certificare a securității cibernetice	**Articolele 85, 86, 88, 89, 90, 92, 93, 94, 95, 96, 97**	ENISA, organismele de evaluare a conformității și autoritățile naționale de certificare a securității cibernetice ar trebui să asigure confidențialitatea datelor și să respecte dispozițiile unui sistem relevant care face trimitere la standardele internaționale și care specifică cerințele.
Date relevante pentru funcțiile interne ale ENISA (buget, DUP, strategii interne)	**Articolul 25** **Articolul 28 alineatul (1)** **Articolul 30** **Articolul 31 alineatul (8)** **Articolul 32 alineatele (3) și (5)**	**Modele și orientări privind reglementarea financiară; orientări interne**

	Articolul 35 alineatele (5) și (6) **Articolele 36-43** **Articolul 44** **Articolul 45** **Articolul 47 alineatul (10)** **Articolele 48-49** **Articolul 52, articolul 58**	
Date cu caracter personal	**Articolul 22** **Titlul II capitolul III secțiunea 6 Comisia pentru soluționarea contestațiilor** **Articolul 66** **Articolul 80 alineatul (1) literele (c), (x)** **Articolul 81 alineatul (2)** **Articolul 88 alineatul (6) litera (h)** **Articolul 95** **Articolul 96**	**Regulamentul (UE) 2018/1725** **Regulamentul (UE) 2016/679**
Date colectate și analizate în contextul efectuării de evaluări coordonate ale riscurilor, al elaborării de scenarii de risc și al identificării activelor TIC esențiale	**Articolul 98** **Articolul 99** **Articolul 102** **Articolul 103** **Articolul 105**	Fără a aduce atingere articolului 13 din Regulamentul (UE) 2024/2847 și articolului 21 din Directiva (UE) 2022/2555

Date privind țările terțe/entitățile din țări terțe	**Articolul 100 alineatele (1), (3), (4)** **Articolul 104** **Articolul 105** **Articolul 107** **Articolul 113**	Nu se aplică
Date privind autoritățile naționale	**Articolul 112** **Articolul 114** **Articolul 116**	Nu se aplică
Date relevante pentru evaluările riscurilor	**Articolul 5 alineatul (2)**	**Standarde de confidențialitate și de gestionare a informațiilor sensibile**
Asistența reciprocă între statele membre	**Articolul 5 alineatul (1) litera (g) din regulament și articolul 1 punctul 12 din directivă**	/

Alinierea la Strategia europeană privind datele

Explicați modul în care cerința (cerințele) este (sunt) aliniată (aliniate) la Strategia europeană privind datele

Cerințele din propunerea CSA2 sunt aliniate fără impact specific în ceea ce privește Strategia europeană privind datele.

Alinierea la principiul înregistrării unice

Explicați modul în care a fost luat în considerare principiul înregistrării unice și cum a fost explorată posibilitatea de a reutiliza datele existente

Unul dintre obiectivele propunerii este de a maximiza eforturile de simplificare ale Comisiei și de a reduce sarcina administrativă pentru statele membre și părțile interesate. În ultimii ani, ENISA a devenit un centru de informare, care deține informații din diferite surse. În acest sens, multe dintre sarcinile ENISA sunt asociate cu reutilizarea și reciclarea informațiilor în scopul diferitelor analize. De exemplu: reutilizarea, în anumite scopuri, a informațiilor notificate în temeiul articolelor 23 și 30 din Directiva (UE) 2022/2555; notificate, partajate sau analizate în temeiul articolului 14 alineatele (1)-(3), al articolului 15 și al articolului 17 alineatele (1) și (3) din Regulamentul (UE) 2024/2847. Dispozițiile cadrului privind lanțul de aprovizionare presupun că punerea sa în aplicare este susținută de datele primite prin articolul 22 din Directiva (UE) 2022/2555, care indică reutilizarea informațiilor și coordonarea.

Explicați modul în care datele nou create sunt ușor de găsit, accesibile, interoperabile și reutilizabile și respectă standarde de înaltă calitate

Propunerea legislativă indică în mod explicit când ar trebui puse datele la dispoziția publicului. Propunerea ia în considerare natura dispozițiilor cu aspecte strict de securitate și confidențialitate și, prin urmare, nu toate datele create în cadrul revizuirii Regulamentului privind securitatea cibernetică vor fi destinate consumului public. În ceea ce privește dispozițiile necesare, a fost asigurată alinierea la portofelul european pentru identitatea digitală. ENISA are sarcina de a oferi servicii de alertă timpurie într-un format prelucrabil automat.

Fluxuri de date

Descriere detaliată a datelor în ceea ce privește domeniul de aplicare și orice standarde/specificații aferente

Tipul de date	**Explicarea fluxului de date**	**Referințe:**

ENISA furnizează rapoarte și analize, orientări tehnice și bune practici.	Acesta este un flux de date care este direcționat către părțile interesate ale ENISA, sprijinind punerea în aplicare a politicii și a legislației UE. În cadrul acestor fluxuri de date, ENISA colectează informații, de cele mai multe ori din surse publice, efectuând analize și partajând rezultatele cu părțile interesate. ENISA execută anumite sarcini și la cererea Comisiei.	Articolul 5 alineatul (1) literele (a), (b), (c), (e), (f), (h) Articolul 5 alineatul (2); Articolul 5 alineatul (3); Articolul 5 alineatul (5) Articolul 6 Articolul 7 Articolul 8 Articolul 9 Articolul 10 Articolul 11 alineatul (2) Articolul 11 alineatul (4) Articolul 14
Fluxurile de date dintre Comisie, ENISA, statele membre și alți actori relevanți din ecosistemul de securitate cibernetică al UE, în sensul cooperării operaționale.	Acest tip de fluxuri de date sunt stabilite în scopul cooperării operaționale și al conștientizării situației. Schimbul de informații se desfășoară în ambele direcții, atât în interior, cât și în exterior. Schimbul se referă la date operaționale.	Articolul 10 alineatul (4) literele (a)-(g) Articolul 11 alineatul (1) literele (b)-(g) Articolul 11 alineatul (2) literele (a), (b) Articolul 11 alineatul (3) Articolul 15 Articolul 16 alineatul (2) litera (e)
Fluxurile de date instituite pentru a sprijini ECSF și sistemele europene de atestare individuală a competențelor în materie de securitate cibernetică și punerea lor în aplicare	Aceste fluxuri de date sprijină schimburile de date în interior și în exterior pentru: - întreținerea și adoptarea ECSF, cu fluxuri între ENISA și membrii grupului său de lucru ad-hoc și între ENISA și Comisie; - dezvoltarea și întreținerea sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică, cu fluxuri între ENISA și membrii grupului său de lucru ad-hoc și între ENISA, Comisie și statele membre; - punerea în aplicare a unor sisteme europene de atestare individuală a competențelor în materie de securitate cibernetică, cu fluxuri de date între solicitanți și ENISA; - fluxuri de date între comisia pentru soluționarea contestațiilor, ENISA, Comisie și solicitanți.	Articolele 19-23 Articolele 36-43

Date relevante pentru obiectivele, scopul și conținutul sistemelor europene de certificare a securității cibernetice	Acest tip de fluxuri de date este relevant pentru planificarea, solicitarea, dezvoltarea, adoptarea și întreținerea (inclusiv posibila revizuire) sistemelor europene de certificare a securității cibernetice. Acesta este legat în special de implicarea și consilierea de specialitate a părților interesate, a ENISA, a autorităților statelor membre prin intermediul ECCG în diferite etape ale procedurii. În plus, fluxurile de date suplimentare sunt legate de furnizarea de informații relevante publicului larg prin intermediul site-urilor dedicate ale Comisiei și ale ENISA. În cele din urmă, cadrul prevede punerea la dispoziția publicului a informațiilor suplimentare în materie de securitate cibernetică de către producătorii sau furnizorii de produse TIC, de servicii TIC sau de procese TIC pentru care s-a eliberat o declarație de conformitate UE sau un certificat european de securitate cibernetică prin mijloace proprii.	Articolul 18 Articolul 19 Articolele 72, 73, 74, 75, 76, 77, 79, 81, 83, 84
Date referitoare la guvernanța cadrului european de certificare a securității cibernetice	Aceste fluxuri de date sprijină schimburile de date în interior și în exterior pentru: - coordonarea și gestionarea sistemelor europene de certificare a securității cibernetice - acreditarea și autorizarea organismelor de evaluare a conformității, precum și notificarea ulterioară a acestora prin intermediul platformei relevante și al procedurilor conexe - proceduri de recurs, cum ar fi dreptul de a depune o plângere, căi de atac judiciare sau proceduri de contestare și de modificare	Articolele 85, 86, 88, 89, 90, 92, 93, 94, 95 și 96

Fluxurile de date legate de activitățile administrative ale agenției	Fluxuri între dintre ENISA, consiliul de administrație, statele membre și Comisie. Informațiile se referă la activitățile administrative ale agenției, în ambele direcții. De asemenea, în unele cazuri se trimit informații Parlamentului European (fluxul de date în acest sens este prezentat mai jos)	Articolul 25 Articolul 28 alineatul (1) Articolul 30 Articolul 31 alineatul (8) Articolul 32 alineatele (3) și (5) Articolul 35 alineatele (5) și (6) Articolele 36-43 Articolul 44 Articolul 45
Date transmise Parlamentului European	Fluxurile către Parlamentul European în ceea ce privește activitățile ENISA și îndeplinirea sarcinilor acesteia; gestiunea bugetară și financiară, cooperarea cu țările terțe și cu organizațiile internaționale, audierea candidatului la funcția de director executiv; aspecte legate de certificarea europeană de securitate cibernetică	Articolul 28 alineatul (1) litera (f), articolul 31 alineatul (8), articolul 32 alineatul (3), articolul 44 alineatul (3), articolul 49 alineatul (6), articolul 49 alineatul (9), articolul 70 alineatul (5), articolul 72 alineatele (4) și (5), articolul 119 alineatul (3) Exercitarea delegării de competențe, articolul 120 Evaluare și revizuire
Date transmise Consiliului UE	Fluxurile către Parlamentul European în ceea ce privește activitățile ENISA și îndeplinirea sarcinilor acesteia; gestiunea bugetară și financiară, cooperarea cu țările terțe și cu organizațiile internaționale, audierea candidatului la funcția de director executiv; propuneri de sisteme în curs de dezvoltare în temeiul cadrului european de certificare a securității cibernetice.	Articolul 28 alineatul (1) litera (f), articolul 31 alineatul (8), articolul 32 alineatul (3), articolul 32 alineatul (7), Articolul 49 alineatul (6), articolul 49 alineatul (9), articolul 70 alineatul (5), articolul 72 alineatele (4), (5), articolul 119 alineatul (3) Exercitarea delegării de competențe, articolul 120 Evaluare și revizuire
Fluxurile de date legate de depunerea unei plângeri	Pentru a gestiona plângerile persoanelor fizice sau juridice în legătură cu certificatele europene de securitate cibernetică eliberate de autoritățile naționale de certificare a securității cibernetice sau cu cele eliberate de organismele de evaluare a conformității în conformitate cu articolul 84 alineatul (4), sau în legătură cu declarațiile de	Articolul 55 alineatul (3); Articolul 88 alineatul (7) litera (f); Articolul 96

	conformitate UE Persoanele fizice sau juridice au dreptul să depună o plângere la entitatea care a eliberat un certificat european de securitate cibernetică sau, dacă plângerea se referă la un certificat european de securitate cibernetică eliberat de un organism de evaluare a conformității.	
Fluxurile de date privind atacurile de tip ransomware	Raportarea anumitor informații în cazul atacurilor de tip ransomware	Articolul 1 punctul 8 din directivă

Tipul de date	**Trimitere (trimiteri) la cerință (cerințe)**	**Actori care furnizează datele**	**Actori care primesc datele**	**Factorul declanșator pentru schimbul de date**	**Frecvența (dacă este cazul)**
Fluxurile de date dintre Comisie și statele membre în contextul efectuării unor evaluări coordonate la nivelul Uniunii ale riscurilor în materie de securitate.	Articolul 99 Evaluările riscurilor în materie de securitate	Comisia și statele membre	Statele membre (Grupul de cooperare NIS)	Articolul 99 Evaluările riscurilor în materie de securitate	Nu se aplică
Fluxurile de date dintre Comisie și Consiliu în legătură cu desemnarea țărilor terțe care prezintă motive de îngrijorare în materie de securitate cibernetică	Articolul 100 Desemnarea țărilor terțe care prezintă motive de îngrijorare	Comisia	Consiliul	Articolul 100 Verificarea de către Comisie a amenințării reprezentate de o	

Tipul de date	Trimitere (trimiteri) la cerință (cerințe)	Actori care furnizează datele	Actori care primesc datele	Factorul declanșator pentru schimbul de date	Frecvența (dacă este cazul)
	în materie de securitate cibernetică			țară terță	
Fluxurile de date dintre Comisie și statele membre în legătură cu măsurile de atenuare în cazul unor circumstanțe excepționale	Articolul 103 alineatul (6) Măsuri de atenuare în cadrul lanțurilor de aprovizionare TIC	Comisia	Statele membre	Situații excepționale	Nu se aplică
Fluxurile de date dintre Comisie și furnizori, pe de o parte, și Comisie și autoritățile competente, pe de altă parte, în ceea ce privește evaluarea stabilirii, a proprietății și a controlului asupra furnizorilor	Articolul 104 alineatele (4), (5), (6) Identificarea furnizorilor cu grad ridicat de risc	Furnizori Comisia Autoritățile competente	Autoritățile competente Furnizori Comisia	Acte de punere în aplicare adoptate în conformitate cu articolul 103 alineatul (1) și în legătură cu interdicția de la articolul 111 alineatul (1)	Nu se aplică
Fluxul de date dintre Comisie și statele membre în ceea ce privește competențele de supraveghere în legătură cu punerea în aplicare a cadrului de securitate a	Articolul 112 alineatele (1), (4)	Statele membre	Comisia	Articolul 112 alineatele (1), (4) Autoritățile	Nu se aplică

Tipul de date	Trimitere (trimiteri) la cerință (cerințe)	Actori care furnizează datele	Actori care primesc datele	Factorul declanșator pentru schimbul de date	Frecvența (dacă este cazul)
lanțului de aprovizionare TIC de încredere	Autoritățile competente Articolul 114 Măsuri de supraveghere și de asigurare a respectării legislației			competente Articolul 114 Măsuri de supraveghere și de asigurare a respectării legislației (Comisia, în cooperare cu statele membre, emite o listă a entităților afiliate furnizorilor cu grad ridicat de risc.)	
Fluxul de date dintre Comisie și părțile terțe pentru derogări	Articolul 105 Derogare pentru entitățile stabilite într-o țară terță sau controlate dintr-o țară terță care prezintă motive de îngrijorare în materie de	Părți terțe [entități stabilite într-o țară terță sau controlate de entități dintr-o țară terță care prezintă motive de îngrijorare în materie de securitate cibernetică (în sensul	Comisia (la primirea cererii de derogare) Părți terțe [entități stabilite într-o țară terță sau controlate de entități dintr-o țară terță care prezintă motive de îngrijorare în	Decizie în temeiul articolului 100 Desemnarea țărilor terțe care prezintă motive de îngrijorare în materie de securitate cibernetică	Nu se aplică

Tipul de date	Trimitere (trimiteri) la cerință (cerințe)	Actori care furnizează datele	Actori care primesc datele	Factorul declanșator pentru schimbul de date	Frecvența (dacă este cazul)
	securitate cibernetică	articolului 100) (atunci când depun o cerere de derogare)] Comisia Europeană (atunci când emite decizii)	materie de securitate cibernetică (în sensul articolului 100) (atunci când primesc decizia Comisiei)]		
Fluxul de date între statele membre și părțile terțe în legătură cu interdicțiile din rețelele de comunicații electronice	Articolul 111 Interdicții privind rețelele de comunicații electronice mobile, fixe și prin satelit	Statele membre (autoritățile competente)	Părți terțe (furnizori de rețele de comunicații electronice mobile, fixe și prin satelit)	Autoritatea competentă desemnată în temeiul prezentului regulament informează fără întârziere autoritatea competentă în temeiul Regulamentului (UE) XX/XXXX [propunerea DNA] cu privire la măsurile impuse furnizorilor de	Nu se aplică

Tipul de date	Trimitere (trimiteri) la cerință (cerințe)	Actori care furnizează datele	Actori care primesc datele	Factorul declanșator pentru schimbul de date	Frecvența (dacă este cazul)
				rețele de comunicații electronice mobile, fixe și prin satelit.	
Fluxul de date între Comisie și statele membre în contextul rețelei pentru cooperare și servicii de sprijin	Articolul 113 Rețeaua pentru cooperare și servicii de sprijin a Comisiei	Comisia Statele membre (autoritățile competente)	Comisia Statele membre (autoritățile competente)	Desemnarea țărilor terțe care prezintă motive de îngrijorare în materie de securitate cibernetică	
Fluxul de date între statele membre și părțile terțe în ceea ce privește măsurile de supraveghere și de asigurare a respectării legislației	Articolul 114 Măsuri de supraveghere și de asigurare a respectării legislației	Părți terțe [entități de tipul celor menționate în anexele I și II la Directiva (UE) 2022/2555]	Statele membre (autoritățile competente)	Punerea în aplicare a măsurilor prevăzute în titlul IV	
Fluxul de date între statele membre pentru asistență reciprocă	Articolul 116 Asistența reciprocă	Statele membre	Statele membre	Dacă o entitate menționată în anexa I sau II din Directiva (UE) 2022/2555 furnizează servicii în mai multe state	Nu se aplică

Tipul de date	Trimitere (trimiteri) la cerință (cerințe)	Actori care furnizează datele	Actori care primesc datele	Factorul declanșator pentru schimbul de date	Frecvența (dacă este cazul)
				membre sau furnizează servicii în unul sau mai multe state membre iar activele TIC esențiale ale acesteia sunt situate în unul sau mai multe alte state membre, autoritățile competente ale statelor membre în cauză cooperează și își oferă asistență reciprocă, după caz.	

4.3. Soluții digitale

Descriere la nivel înalt a soluțiilor digitale

Pentru fiecare soluție digitală, explicația modului în care soluția digitală respectă politicile digitale și actele legislative aplicabile

Soluția digitală	Trimitere (trimiteri) la cerință (cerințe)	Principalele funcționalități obligatorii	Organismul responsabil	Cum este asigurată accesibilitatea?	Cum se ia în considerare potențialul de reutilizare?	Utilizarea tehnologiilor IA (dacă este cazul)

ENISA, asigurând **secretariatul rețelei CSIRT și al EU-CyCLONe** și utilizând în cadrul rețelei CSIRT și EU-CyCLONe **instrumente securizate de comunicații** care sunt furnizate de entități juridice care nu sunt stabilite în țări terțe sau controlate de țări terțe sau de resortisanți ai țărilor terțe.	Articolul 10 alineatele (2), (3), (5)	Informații fără caracter public	ENISA	Informații fără caracter public	Informații fără caracter public	Informații fără caracter public
Dezvoltă, în cooperare cu EU-CyCLONe, rețeaua CSIRT, Comisia, Europol și CERT-UE și entități relevante ale Uniunii, **registre de informații verificate și fiabile privind amenințările cibernetice**, inclusiv tendințele în materie de incidente, tactici, tehnici și proceduri.	Articolul 11 alineatul (1) litera (a)	informații verificate și fiabile privind amenințările cibernetice, inclusiv tendințele în materie de incidente, tactici, tehnici și proceduri	ENISA EU-CyCLONe, rețeaua CSIRT, Comisia, Europol și CERT-UE și entitățile relevante ale Uniunii	Nu se aplică	Nu se aplică	Nu se aplică
ENISA **păstrează un registru al învățămintelor desprinse.**	Articolul 14 alineatul (2)	ENISA menține un registru al învățămintelor desprinse în urma exercițiilor și recomandă statelor membre și, după caz, entităților Uniunii modul în care pot fi puse în aplicare în mod eficace și eficient învățămintele desprinse.	ENISA	Nu se aplică	Nu se aplică	Nu se aplică

ENISA instituie, furnizează, operează, întreține și actualizează, după caz, instrumente tehnice operaționale, cum ar fi **platforme** legate de securitatea cibernetică la nivelul Uniunii, în special platforma unică de raportare instituită în temeiul articolului 16 alineatul (1) din Regulamentul (UE) 2024/2847 [și punctul unic de intrare pentru raportarea incidentelor instituit în temeiul articolului 23a din Directiva (UE) 2022/2555] sau instrumente de testare pentru a sprijini punerea în aplicare a procedurilor de evaluare a conformității în conformitate cu legislația relevantă a Uniunii.	Articolul 15	Platforma unică de raportare Articolul 16 alineatul (1) din Regulamentul (UE) 2024/2847 [punct unic de intrare Articolul 23a din Directiva (UE) 2022/2555]	ENISA	Nu se aplică	Nu se aplică	Nu se aplică
Întreține baza de date europeană a vulnerabilităților instituită în temeiul articolului 12 alineatul (2) din Directiva (UE) 2022/2555 și **furnizează servicii de gestionare a vulnerabilităților**	Articolul 16 alineatul (2)	Articolul 12 alineatul (2) din Directiva (UE) 2022/2555 Întreținerea bazei de date și furnizarea de servicii de gestionare a vulnerabilităților	ENISA	Nu se aplică	Nu se aplică	Nu se aplică
ENISA menține și actualizează periodic un site dedicat care oferă informații publice	Articolele 19-23	Menține și actualizează periodic un site dedicat care oferă informații publice cu privire la ECSF, inclusiv cadrul și calendarul de actualizare a acestuia; sistemele europene de atestare	ENISA	Nu se aplică	Nu se aplică	Nu se aplică

		individuală a competențelor în materie de securitate cibernetică, progresele înregistrate de acestea și termenele pentru dezvoltarea lor; taxele asociate fiecărui sistem european de atestare individuală a competențelor în materie de securitate cibernetică; costul orientativ al unui atestat european individual de competențe în materie de securitate cibernetică; lista furnizorilor de atestate autorizați.				
Comisia menține și actualizează periodic un site public dedicat	Articolul 72	Următoarele informații: (a) Sistemele europene de certificare a securității cibernetice a căror dezvoltare este solicitată; (b) prioritățile strategice pentru armonizarea produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate sau a cerințelor	Comisia Europeană	Respectarea orientărilor	Respectarea orientărilor	Nu se aplică

		de securitate din legislația Uniunii, inclusiv domeniile potențiale pentru care ar putea fi solicitat un sistem european de certificare a securității cibernetice.				
ENISA menține un site dedicat certificării	Articolul 79	Furnizarea de informații cu privire la: (a) sistemele europene de certificare a securității; (b) taxele aferente întreținerii fiecărui sistem european de certificare a securității cibernetice; (c) specificațiile tehnice relevante ale ENISA; (d) certificatele europene de securitate cibernetică și declarațiile de conformitate UE, inclusiv informații cu privire la certificatele și declarațiile care nu mai sunt valabile sau care sunt suspendate, retrase sau expirate; (e) informațiile suplimentare relevante în materie de securitate	ENISA	Respectarea orientărilor	Respectarea orientărilor	Nu se aplică

		cibernetică furnizate în conformitate cu articolul 84 alineatul (2); (f) rezumatele evaluărilor *inter pares* în temeiul articolului 89 alineatul (7); (g) specificațiile tehnice menționate într-un sistem european de certificare a securității cibernetice în temeiul articolului 74 alineatul (10).				
Registrul (derogărilor pentru entitățile stabilite într-o țară terță sau controlate de entități dintr-o țară terță care prezintă motive de îngrijorare în materie de securitate cibernetică)	Articolul 107 Registrul	Comisia ține un registru accesibil publicului cu deciziile sale menționate la articolul 105 alineatul (4). Registrul menționează numele entităților care au făcut obiectul deciziilor. Comisia îl actualizează periodic.	Comisia	„Comisia ține un registru accesibil publicului”	Nu se aplică	Nu se aplică

Platformă (pentru cooperare și schimb de informații între Comisie și autoritățile competente)	Articolul 113	Comisia instituie o rețea de cooperare a autorităților competente ale statelor membre și a Comisiei, care să servească drept platformă pentru cooperare și schimb de informații. Comisia oferă sprijin administrativ rețelei.	Comisia	Nu sunt publice, numai pentru autoritățile competente	Nu se aplică	Nu se aplică
ENISA creează și menține un registru al entităților esențiale și importante, precum și al entităților care furnizează servicii de înregistrare a numelor de domenii	Articolul 1 punctul 11 din directivă	Registrul entităților esențiale și importante, precum și al entităților care furnizează servicii de înregistrare a numelor de domenii	ENISA	Nu se aplică	Pe baza informațiilor primite de la punctele unice de contact în conformitate cu alineatul (2). (Articolul 27 din Directiva NIS 2)	Nu se aplică

Soluții digitale incluse în tabelul de mai sus

Politica digitală și/sau sectorială (atunci când	**Explicarea modului în care se aliniază**

sunt aplicabile)	
Regulamentul privind IA	Nu se aplică
Cadrul UE privind securitatea cibernetică	Nu se aplică
eIDAS	Nu se aplică
Portalul digital unic și IMI	Nu se aplică
Altele	Nu se aplică

Descriere la nivel înalt a serviciului (serviciilor) public(e) digital(e) afectat(e) de cerințe

Serviciul public digital sau categoria de servicii publice digitale	**Descriere**	**Trimitere (trimiteri) la cerință (cerințe)**	**Soluție (soluții) pentru Europa interoperabilă (NU SE APLICĂ)**	**Altă (alte) soluție (soluții) de interoperabilitate**
ENISA în calitate de secretariat al rețelelor și care implementează instrumente de comunicare securizate	ENISA asigură secretariatul rețelei CSIRT în temeiul articolului 15 alineatul (2) din Directiva (UE) 2022/2555. ENISA asigură secretariatul EU-CyCLONe în temeiul articolului 16 alineatul (2) din Directiva (UE) 2022/2555 [și punctul unic de intrare pentru raportarea incidentelor instituit în temeiul articolului 23a din Directiva (UE) 2022/2555], precum și instrumente de testare pentru a sprijini punerea în aplicare a procedurilor de evaluare a conformității în conformitate cu legislația relevantă a Uniunii.	Articolul 11	//	Nu se aplică

	ENISA implementează, în cadrul rețelei CSIRT și al EU-CyCLONe, instrumente securizate de comunicații care sunt furnizate de entități juridice care nu sunt stabilite în țări terțe sau controlate de țări terțe sau de resortisanți ai țărilor terțe.			
Alerte timpurii	Emiterea de alerte timpurii	Articolul 11 Articolul 12		
Sprijin în legătură cu un anumit incident sau amenințare cibernetică potențial(ă) sau în curs	La cererea unuia sau mai multor state membre, furnizarea de consiliere și evaluări în legătură cu un anumit incident potențial sau în curs sau cu o anumită amenințare cibernetică, inclusiv prin furnizarea de expertiză și prin facilitarea gestionării tehnice a unor astfel de incidente, precum și prin sprijinirea schimbului voluntar de informații relevante și de soluții tehnice între statele membre;	Articolul 10		
Sprijinirea gestionării coordonate a incidentelor și crizelor de securitate cibernetică de mare amploare la nivel operațional	Contribuția la sprijinirea gestionării coordonate a incidentelor și a crizelor de securitate cibernetică de mare amploare la nivel operațional, în special prin sprijinirea EU-CyCLONe în pregătirea rapoartelor către nivelul politic și prin facilitarea schimbului de informații în timp util între rețeaua CSIRT și EU-CyCLONe.	Articolul 10		
Registre de informații verificate și fiabile privind amenințările cibernetice	Dezvoltă, în cooperare cu EU-CyCLONe, rețeaua CSIRT, Comisia, Europol și CERT-UE și entități relevante ale Uniunii, registre de informații verificate și fiabile privind amenințările cibernetice, inclusiv tendințele în materie de incidente,	Articolul 11		

	tactici, tehnici şi proceduri.			
Registrul învățămintelor desprinse	ENISA menține un registru al învățămintelor desprinse în urma exercițiilor respective și recomandă statelor membre și, după caz, entităților Uniunii modul în care pot fi puse în aplicare în mod eficace și eficient învățămintele desprinse.	Articolul 14		
ENISA instituie, furnizează, operează, întreține și actualizează, după caz, instrumente tehnice operaționale, cum ar fi platformele	ENISA instituie, furnizează, operează, întreține și actualizează, după caz, instrumente tehnice operaționale, cum ar fi platforme legate de securitatea cibernetică la nivelul Uniunii, în special platforma unică de raportare instituită în temeiul articolului 16 alineatul (1) din Regulamentul (UE) 2024/2847 [și punctul unic de intrare pentru raportarea incidentelor instituit în temeiul articolului 23a din Directiva (UE) 2022/2555], precum și instrumente de testare pentru a sprijini punerea în aplicare a procedurilor de evaluare a conformității în conformitate cu legislația relevantă a Uniunii.	Articolul 15		
Întreținerea bazei de date europene a vulnerabilităților instituite în temeiul articolului 12 alineatul (2) din Directiva (UE) 2022/2555.	Întreținerea bazei de date europene a vulnerabilităților instituite în temeiul articolului 12 alineatul (2) din Directiva (UE) 2022/2555. Furnizarea de servicii de gestionare a vulnerabilităților către părțile interesate, pe baza bazei de date europene a vulnerabilităților și utilizând informațiile relevante aflate la dispoziția ENISA. Inițierea unei cooperări structurate cu organizații care furnizează programe,	Articolul 16		

	registre sau baze de date similare cu baza de date europeană a vulnerabilităților. Sprijinirea activă a echipelor CSIRT desemnate drept coordonatori în temeiul articolului 12 alineatul (1) din Directiva (UE) 2022/2555 în ceea ce privește gestionarea divulgării coordonate a vulnerabilităților care pot avea un impact semnificativ asupra entităților din mai multe state membre. Dezvoltarea și menținerea metodologiilor și a mecanismelor de guvernanță pentru identificarea vulnerabilităților și divulgarea coordonată, în cooperare cu autoritățile naționale competente, echipele CSIRT, industria și comunitatea de cercetare.			
Pregătirea propunerilor de sisteme europene de certificare a securității cibernetice	Pregătirea propunerilor de sisteme europene de certificare a securității cibernetice („propuneri de sisteme”) pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura de securitate cibernetică a entităților și specificațiile tehnice aferente în conformitate cu articolul 74. Întreținerea sistemelor europene de certificare a securității cibernetice adoptate în conformitate cu articolul 75, inclusiv în vederea unei posibile revizuiri a sistemelor europene de certificare a securității cibernetice adoptate în conformitate cu articolul 76.	Articolul 17		
ENISA elaborează și	ENISA elaborează și întreține sisteme	Articolele 20-22		

întreține sisteme europene de atestare individuală a competențelor în materie de securitate cibernetică	europene de atestare individuală a competențelor în materie de securitate cibernetică ENISA emite o decizie motivată prin care acordă solicitantului autorizația de a elibera atestate individuale europene pentru furnizarea și întreținerea sistemelor și a autorizației sau prin care nu acordă autorizația sau prin care închide prelucrarea cererii din cauza informațiilor insuficiente furnizate de solicitant sau din cauza lipsei de acțiune a acestuia în urma unei cereri de informații suplimentare.			
ENISA menține și actualizează periodic un site dedicat.	ENISA menține și actualizează periodic un site dedicat care oferă informații publice cu privire la: (a) ECSF, inclusiv cadrul și calendarul de actualizare a acestuia; (b) sistemele europene de atestare individuală a competențelor în materie de securitate cibernetică, progresele înregistrate de acestea și termenele pentru dezvoltarea lor; (c) taxele asociate fiecărui sistem european de atestare individuală a competențelor în materie de securitate cibernetică adoptat în temeiul articolului 47 din prezentul regulament; (d) costul orientativ al unui atestat european individual de competențe în materie de securitate cibernetică în conformitate cu articolul 20 alineatul (4); (e) lista furnizorilor de atestate	Articolul 23		

	autorizați.			
Comisia menține și actualizează periodic un site public dedicat	Comisia menține și actualizează periodic un site dedicat care oferă informații cu privire la următoarele aspecte: (a) sistemele europene de certificare a securității cibernetice a căror dezvoltare este solicitată; (b) prioritățile strategice pentru armonizarea produselor TIC, a serviciilor TIC, a proceselor TIC, a serviciilor de securitate gestionate sau a cerințelor de securitate din legislația Uniunii, inclusiv domeniile potențiale pentru care ar putea fi solicitat un sistem european de certificare a securității cibernetice.	Articolul 72		
ENISA menține un site dedicat certificării	ENISA menține și actualizează periodic un site dedicat care oferă informații publice cu privire la următoarele: (a) sistemele europene de certificare a securității; (b) taxele aferente întreținerii fiecărui sistem european de certificare a securității cibernetice; (c) specificațiile tehnice relevante ale ENISA; (d) certificatele europene de securitate cibernetică și declarațiile de conformitate UE, inclusiv informații cu privire la certificatele și declarațiile care nu mai sunt valabile sau care sunt suspendate, retrase sau expirate; (e) informațiile suplimentare relevante în materie de securitate cibernetică	Articolul 79		

	furnizate în conformitate cu articolul 84 alineatul (2); (f) rezumatele evaluărilor *inter pares* în temeiul articolului 89 alineatul (7); (g) specificațiile tehnice menționate într-un sistem european de certificare a securității cibernetice în temeiul articolului 74 alineatul (10).			
Investigații	Comisia investighează toate cazurile în care are îndoieli sau i se aduc la cunoștință îndoieli cu privire la competența unui organism de evaluare a conformității de a îndeplini cerințele și responsabilitățile care îi revin sau la continuarea îndeplinirii acestora de către un organism de evaluare a conformității. Comisia se asigură că toate informațiile sensibile obținute pe parcursul investigațiilor sale sunt tratate în mod confidențial.	Articolul 94		
ENISA creează și menține un registru al entităților esențiale și importante, precum și al entităților care furnizează servicii de înregistrare a numelor de domenii	Registrul entităților esențiale și importante, precum și al entităților care furnizează servicii de înregistrare a numelor de domenii La cerere, ENISA permite autorităților competente accesul la informații privind furnizorii de servicii DNS, registrele de nume TLD, entitățile care furnizează servicii de înregistrare a numelor de domenii, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, precum și furnizorii de piețe online, de motoare de căutare	Articolul 1 punctul 11 din directivă		

	online și de platforme de servicii de socializare în rețea stocați în registrul respectiv, asigurându-se, în același timp, că este protejată confidențialitatea informațiilor, după caz.			

4.4. Evaluarea interoperabilității

Impactul cerinței (cerințelor) asupra interoperabilității transfrontaliere din perspectiva serviciului public digital

Registrele/platforme/alerte timpurii/secretariat/cooperare operațională/bază de date CVD

Evaluare	Măsuri	Obstacole potențiale rămase
Evaluarea alinierii la politicile digitale și sectoriale existente **Vă rugăm să enumerați politicile digitale și sectoriale aplicabile identificate**	*Securitatea cibernetică*	*Nu există bariere cunoscute*
Evaluați măsurile organizatorice în vederea unei furnizări transfrontaliere fără probleme a serviciilor publice digitale **Vă rugăm să enumerați măsurile de guvernanță prevăzute**	*Consiliul de administrație al ENISA* *Rețeaua CSIRT* *EU-CyCLONe* *Grupul de cooperare NIS* *Toate acestea sunt forumuri în care pot fi ridicate probleme.*	*Nu se aplică*
Evaluarea măsurilor luate pentru a asigura o înțelegere comună a datelor **Vă rugăm să enumerați astfel de măsuri**	*Nu se aplică*	*Nu se aplică*
Evaluați utilizarea specificațiilor și standardelor tehnice deschise convenite de comun acord	*Nu se aplică*	*Nu se aplică*

Vă rugăm să enumerați astfel de măsuri		

Sisteme europene de atestare individuală a competențelor în materie de securitate cibernetică

Evaluare	Măsuri	Obstacole potențiale rămase
Evaluarea alinierii la politicile digitale și sectoriale existente **Vă rugăm să enumerați politicile digitale și sectoriale aplicabile identificate**	*Propunerea se bazează pe COM(2023) 207 final (Academia de competențe în materie de securitate cibernetică): „ENISA va elabora un proiect-pilot care va explora instituirea unui sistem european de atestare a competențelor în materie de securitate cibernetică”* *Aceasta utilizează Regulamentul (UE) 2024/1183 (portofelul EUDI) stabilind că „ENISA și furnizorii de atestate autorizați se asigură că atestatele electronice ale atestatului european individual de competențe în materie de securitate cibernetică sunt eliberate portofelelor europene pentru identitatea digitală”* *Securitatea cibernetică* *RGPD (păstrarea evidențelor de către furnizori)*	*Nu există bariere cunoscute*
Evaluați măsurile organizatorice în vederea unei furnizări transfrontaliere fără probleme a serviciilor publice digitale **Vă rugăm să enumerați măsurile de guvernanță prevăzute**	*Consultarea părților interesate atunci când se pregătește un sistem european de atestare individuală a competențelor în materie de securitate cibernetică* *Separarea activităților în cadrul ENISA pentru a asigura desfășurarea independentă a acestora* *Comisia pentru soluționare a contestațiilor*	*Utilizarea și recunoașterea sistemelor europene de atestare individuală a competențelor în materie de securitate cibernetică rămân voluntare pentru entitățile publice și private.*
Evaluarea măsurilor luate pentru a		*Deși sistemele ar trebui să fie la fel de detaliate încât să*

asigura o înțelegere comună a datelor **Vă rugăm să enumerați astfel de măsuri**	*Elaborarea de sisteme care detaliază, printre altele, normele privind conținutul și formatul atestărilor* *Furnizorii autorizați se asigură că, la cererea persoanei fizice, atestatele electronice ale atestatelor europene individuale de competențe în materie de securitate cibernetică sunt emise ca atestate electronice ale atributelor într-un format care poate fi stocat în portofelele europene pentru identitatea digitală. ENISA va oferi orientări evaluatorilor și va efectua formarea obligatorie a acestora în ceea ce privește cerințele și metodele de evaluare incluse în sistemul de atestare europeană individuală a competențelor în materie de securitate cibernetică.* *Furnizarea de informații publice pe un site* Acte de punere în aplicare privind taxele	*asigure o înțelegere comună și să faciliteze punerea în aplicare și deși ENISA va oferi orientări evaluatorilor și va desfășura o formare obligatorie a acestora pentru a asigura punerea în aplicare coerentă a sistemelor, ar putea apărea dimensiuni neprevăzute în cazul în care furnizorii de atestate autorizați trebuie să interacționeze cu ENISA, cu alți furnizori sau evaluatori.*
Evaluați utilizarea specificațiilor și standardelor tehnice deschise convenite de comun acord **Vă rugăm să enumerați astfel de măsuri**	*Sistemele europene de atestare individuală a competențelor în materie de securitate cibernetică sunt elaborate cu sprijinul părților interesate relevante*	*Nu se aplică*

Pregătirea propunerilor de sisteme europene de certificare a securității cibernetice/atribuirea numerelor către organismele de evaluare a conformității

Evaluare	Măsuri	Obstacole potențiale rămase
Evaluarea alinierii la politicile digitale și sectoriale existente **Vă rugăm să enumerați politicile digitale și sectoriale aplicabile**	*Propunerea urmărește alinierea în materie de guvernanță la noul cadru legislativ, în special în ceea ce privește Regulamentul (CE) nr. 765/2008*[26]*.*	*Nu există bariere cunoscute*

identificate	*Propunerea urmărește să faciliteze respectarea legislației sectoriale relevante în materie de securitate cibernetică prin dezvoltarea unor sisteme europene de certificare a securității cibernetice specifice.*	
Evaluați măsurile organizatorice în vederea unei furnizări transfrontaliere fără probleme a serviciilor publice digitale **Vă rugăm să enumerați măsurile de guvernanță prevăzute**	*Grupul european pentru certificarea securității cibernetice;* *ENISA;* *Grupuri de lucru ad-hoc;* *Adunarea europeană pentru certificarea securității cibernetice;* *Consultarea părților interesate atunci când solicită, elaborează și adoptă sisteme europene de certificare a securității cibernetice;* *Proceduri de comitologie pentru actele de punere în aplicare avute în vedere referitoare la sistemele europene de certificare a securității cibernetice.*	*Utilizarea certificării europene de securitate cibernetică este voluntară, cu excepția cazului în care se prevede altfel în legislația europeană.*
Evaluarea măsurilor luate pentru a asigura o înțelegere comună a datelor **Vă rugăm să enumerați astfel de măsuri**	*Actele de punere în aplicare enumerate în secțiunea 4.5.*	*Utilizarea certificării europene de securitate cibernetică este voluntară, cu excepția cazului în care se prevede altfel în legislația europeană.*
Evaluați utilizarea specificațiilor și standardelor tehnice deschise convenite de comun acord **Vă rugăm să enumerați astfel de măsuri**	*Actele de punere în aplicare enumerate în secțiunea 4.5.* *Cerințele specificate ale sistemului european de certificare a securității cibernetice trebuie să fie conforme cu cerințele legislației Uniunii.* *Sistemele europene de certificare a securității cibernetice valorifică și fac trimitere la standardele internaționale, europene sau naționale aplicate în cadrul evaluării sau, în cazul în care astfel de standarde nu sunt disponibile sau adecvate, la specificațiile*	*Nu se aplică*

	tehnice elaborate de ENISA.	

Site-uri accesibile publicului

Evaluare	Măsuri	Obstacole potențiale rămase
Evaluarea alinierii la politicile digitale și sectoriale existente **Vă rugăm să enumerați politicile digitale și sectoriale aplicabile identificate**	*Regulamentul UE privind accesibilitatea și* *Directiva privind accesibilitatea site-urilor* *Securitatea cibernetică*	*Nu există bariere cunoscute*
Evaluați măsurile organizatorice în vederea unei furnizări transfrontaliere fără probleme a serviciilor publice digitale **Vă rugăm să enumerați măsurile de guvernanță prevăzute**	*Nu se aplică*	*Nu se aplică*
Evaluarea măsurilor luate pentru a asigura o înțelegere comună a datelor **Vă rugăm să enumerați astfel de măsuri**		*Nu se aplică*
Evaluați utilizarea specificațiilor și standardelor tehnice deschise convenite de comun acord **Vă rugăm să enumerați astfel de măsuri**		*Nu se aplică*

4.5. Măsuri de sprijinire a implementării digitale

Descriere la nivel înalt a măsurilor de sprijinire a implementării digitale

Descrierea măsurii	**Trimitere (trimiteri) la cerință (cerințe)**	**Rolul Comisiei** (dacă este cazul)	**Actorii care urmează să fie**	**Calendarul preconizat** (dacă este cazul)

			implicați (dacă este cazul)	
Pe baza propunerii de sistem acceptate pregătite de ENISA, Comisia este împuternicită să adopte acte de punere în aplicare care să prevadă un sistem european de certificare a securității cibernetice pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate sau postura de securitate cibernetică a entităților care îndeplinesc cerințele prevăzute la articolele 80 și 81. Acest act de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2).	Articolul 75 alineatul (9)	Comisia este împuternicită să adopte acte de punere în aplicare		Nu se aplică
Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 119 pentru a modifica alineatul (1) de la prezentul articol prin adăugarea sau modificarea obiectivelor de securitate, pentru a se asigura că acestea reflectă cele mai recente evoluții tehnologice și noile amenințări conexe, precum și prin adoptarea unei noi legislații a Uniunii care să stabilească prezumția de conformitate prin certificarea europeană de securitate cibernetică cu cerințele de securitate cibernetică relevante din legislația respectivă.	Articolul 80 alineatul (2)	Comisia este împuternicită să adopte acte delegate		Nu se aplică
Comisia este împuternicită să adopte acte	Articolul 81 alineatul (5)	Comisia este	ENISA	Nu se aplică

de punere în aplicare de stabilire a unor principii comune și a unor modele de dispoziții pentru elementele prevăzute la alineatele (1), (2) și (3) în cadrul sistemelor europene de certificare a securității cibernetice. Dacă este cazul și dacă este disponibil, un sistem european de certificare a securității cibernetice poate include trimiteri la aceste principii și modele de dispoziții. Actele de punere în aplicare menționate la primul paragraf se adoptă în conformitate cu procedura de examinare prevăzută la articolul 118 alineatul (2). Atunci când elaborează sau revizuiește principiile comune și modelele de dispoziții pentru elementele sistemelor europene de certificare a securității cibernetice, Comisia consultă ENISA și ia în considerare, după caz, opiniile exprimate de ECCG, de părțile interesate relevante și de alte organisme relevante.		împuternicită să adopte acte de punere în aplicare	ECCG	
Comisia este împuternicită să adopte acte de punere în aplicare care să precizeze procedurile de aprobare prealabilă sau modelele generale de delegare menționate la alineatul (4) de la prezentul articol. În procesul de elaborare a respectivelor acte de punere în aplicare, Comisia consultă ECCG. Respectivele acte de punere în	Articolul 85 alineatul (5)	Comisia este împuternicită să adopte acte de punere în aplicare	ECCG	Nu se aplică

aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2).				
Certificatele țărilor terțe pentru produsele TIC, serviciile TIC, procesele TIC, serviciile de securitate gestionate și postura de securitate cibernetică a entităților pot fi recunoscute, prin intermediul unui act de punere în aplicare sau prin încheierea unui acord între Uniune și țara terță în cauză sau o organizație internațională, ca fiind echivalente cu certificatele europene de securitate cibernetică în cazul în care cerințele sistemului relevant al țării terțe sau ale sistemului relevant al organizației internaționale sunt considerate echivalente cu cele ale sistemelor europene de certificare a securității cibernetice. Comisia este împuternicită să adopte astfel de acte de punere în aplicare. Actele de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2).	Articolul 87 alineatul (1)	Comisia este împuternicită să adopte acte de punere în aplicare		Nu se aplică
Comisia este împuternicită să adopte acte de punere în aplicare prin care să stabilească un plan pentru evaluarea *inter pares*, care acoperă o perioadă de cel puțin cinci ani, și să definească criterii privind componența echipei de evaluare *inter*	Articolul 89 alineatul (6)	Comisia este împuternicită să adopte acte de punere în aplicare		Nu se aplică

pares, metodologia utilizată pentru evaluarea *inter pares*, calendarul, frecvența și alte atribuții legate de evaluarea *inter pares*. La elaborarea respectivelor acte de punere în aplicare, Comisia consultă ECCG și ENISA. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2).				
Comisia este împuternicită să adopte acte de punere în aplicare pentru a stabili procedurile, inclusiv în ceea ce privește cooperarea transfrontalieră, de autorizare a organismelor de evaluare a conformității. În procesul de elaborare a actelor de punere în aplicare, Comisia consultă ENISA și ECCG. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2).	Articolul 92 alineatul (8)	Comisia este împuternicită să adopte acte de punere în aplicare	ENISA ECCG	Nu se aplică
Comisia este împuternicită să adopte acte de punere în aplicare pentru a stabili circumstanțele, formatele și procedurile pentru notificările menționate la alineatul (1) de la prezentul articol, inclusiv procedura de opoziție a altor state membre în cursul procesului de notificare, identificarea unică a organismelor de evaluare a conformității, precum și circumstanțele pentru restricționarea, suspendarea sau retragerea notificării.	Articolul 93 alineatul (3)	Comisia este împuternicită să adopte acte de punere în aplicare		Nu se aplică

Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2).				
Comisia poate adopta acte de punere în aplicare în conformitate cu articolul 100 pentru a desemna o țară terță care prezintă motive de îngrijorare în materie de securitate cibernetică la nivelul lanțurilor de aprovizionare TIC.	Articolul 100 alineatul (2) Desemnarea țărilor terțe care prezintă motive de îngrijorare în materie de securitate cibernetică	Adoptarea actelor de punere în aplicare		Nu se aplică Nu există un calendar, dar actele de punere în aplicare ar trebui revizuite periodic
Comisia poate adopta acte de punere în aplicare pentru a prevedea una sau mai multe măsuri de atenuare menționate la articolul 103 alineatul (2).	Articolul 103 alineatul (2) Măsuri de atenuare în cadrul lanțului de aprovizionare TIC	Adoptarea actelor de punere în aplicare	Nu se aplică	Nu se aplică Nu există un calendar, dar urmează să fie revizuite o dată la 36 de luni [în conformitate cu procedura de examinare menționată la articolul 118 alineatul (2)]
Comisia poate adopta acte de punere în aplicare în conformitate cu articolul 102 pentru a identifica active TIC esențiale utilizate pentru fabricarea de produse sau furnizarea de servicii de către tipurile de entități menționate în anexele I și II la Directiva (UE) 2022/2555.	Articolul 102 alineatul (1) Identificarea activelor TIC esențiale	Adoptarea actelor de punere în aplicare	Nu se aplică	Nu se aplică
Comisia poate adopta acte de punere în	Articolul 103 alineatul (1)	Adoptarea actelor	Nu se aplică	Nu se aplică

aplicare prin care să interzică utilizarea, instalarea sau integrarea sub orice formă a componentelor TIC sau a componentelor care includ componente TIC de la furnizori cu grad ridicat de risc, astfel cum sunt desemnați în conformitate cu articolul 100 alineatul (2), în activele TIC esențiale identificate în conformitate cu articolul 102.	Măsuri de atenuare în cadrul lanțului de aprovizionare TIC	de punere în aplicare		
Comisia poate adopta acte de punere în aplicare pentru a stabili că entităților de tipurile menționate în anexele I și II la Directiva (UE) 2022/2555 li se interzice să utilizeze, să instaleze sau să integreze componente TIC sau componente care includ componente TIC de la o anumită entitate.	Articolul 103 alineatul (7)	Adoptarea actelor de punere în aplicare	Consultarea statelor membre și a entităților în cauză	Nu se aplică
Prin intermediul unor acte de punere în aplicare, Comisia stabilește liste cu furnizorii cu grad ridicat de risc relevanți pentru interdicțiile prevăzute în actele de punere în aplicare adoptate în conformitate cu articolul 103 alineatul (1) sau pentru interdicția menționată la articolul 111 alineatul (1).	Articolul 104 alineatul (1)	Adoptarea actelor de punere în aplicare	Nu se aplică	Nu se aplică
Comisia poate adopta acte de punere în aplicare pentru a detalia condițiile menționate la articolul 105 alineatul (2) litera (b) și pentru a stabili norme detaliate cu privire la procedurile menționate la articolul 105.	Articolul 105 Derogare pentru entitățile stabilite într-o țară terță sau controlate de entități dintr-o țară terță care prezintă motive de îngrijorare în	Adoptarea actelor de punere în aplicare	Nu se aplică	Nu se aplică

	materie de securitate cibernetică			
Comisia poate adopta acte de punere în aplicare prin care stabilește norme detaliate privind taxele, precizând cuantumul taxelor și modalitatea de plată a acestora.	Articolul 109 Taxe	Adoptarea actelor de punere în aplicare	Nu se aplică	Nu se aplică
Comisia adoptă acte de punere în aplicare pentru a specifica perioadele de timp pentru eliminarea treptată a componentelor TIC sau a componentelor care includ componente TIC furnizate de furnizori cu grad ridicat de risc în ceea ce privește rețelele de comunicații electronice fixe și prin satelit.	Articolul 110 alineatul (4) Activele TIC esențiale pentru rețelele de comunicații electronice mobile, fixe și prin satelit	Adoptarea actelor de punere în aplicare	Nu se aplică	Nu se aplică
Comisia poate adopta acte delegate în conformitate cu articolul 119 pentru a modifica anexa II în vederea adaptării acesteia la evoluțiile tehnologice, ținând seama de elementele menționate la articolul 103 alineatul (3).	Articolul 110 alineatul (5)	Adoptarea actelor delegate	Nu se aplică	Nu se aplică
7. Articolul 21 alineatul (5) se modifică după cum urmează: (a) al doilea paragraf se înlocuiește cu următorul text: „Comisia poate adopta acte de punere în aplicare de stabilire a cerințelor tehnice și metodologice, precum și a cerințelor sectoriale, după caz, ale măsurilor menționate la alineatul (2) în ceea ce privește entitățile esențiale și entitățile importante, altele decât cele menționate la	Articolul 1 punctul 7 din directivă Armonizarea maximă	Comisia poate adopta acte de punere în aplicare		Nu se aplică

primul paragraf de la prezentul alineat. Comisia evaluează periodic dacă actele de punere în aplicare menționate la prezentul paragraf se adoptă pentru anumite sectoare sau tipuri de entități pentru a îmbunătăți funcționarea pieței interne. Pe baza rezultatelor acestor evaluări, Comisia poate propune astfel de acte de punere în aplicare pentru sectoarele sau tipurile de entități identificate. Atunci când pregătește aceste evaluări, Comisia se axează în special pe caracterul transfrontalier al sectoarelor sau al tipurilor de entități și desfășoară un proces de consultare deschis, transparent și cuprinzător cu părțile interesate relevante și cu statele membre.”; (b) următorul paragraf se introduce după al patrulea paragraf: „În cazul în care Comisia adoptă actele de punere în aplicare menționate la primul și al doilea paragraf de la prezentul alineat, statele membre nu trebuie să impună entităților care intră în domeniul de aplicare al respectivelor acte de punere în aplicare nicio cerință tehnică dau metodologică suplimentară legată de măsurile menționate la articolul 21 alineatul (2) din Directiva (UE) 2022/2555.”				