Consiliul
Uniunii Europene

Bruxelles, 22 martie 2022
(OR. en)

7474/22

Dosar interinstituțional:
2022/0085 (COD)

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

PROPUNERE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	22 martie 2022
Destinatar:	Dl Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2022) 122 final
Subiect:	Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii

În anexă, se pune la dispoziția delegațiilor documentul COM(2022) 122 final.

Anexă: COM(2022) 122 final

COMISIA
EUROPEANĂ

Bruxelles, 22.3.2022
COM(2022) 122 final

2022/0085 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii

{SWD(2022) 67 final} - {SWD(2022) 68 final}

EXPUNERE DE MOTIVE

1. CONTEXT

• Motivele și obiectivele propunerii

Prezenta propunere stabilește un cadru pentru asigurarea unor norme și măsuri comune în materie de securitate cibernetică în rândul instituțiilor, organelor și agențiilor Uniunii. Scopul său este de a îmbunătăți în continuare capacitățile de reziliență și de răspuns la incidente ale tuturor entităților. Propunerea reflectă prioritățile Comisiei de a pregăti Europa pentru era digitală și de a construi o economie capabilă să facă față provocărilor viitorului și aflată în serviciul cetățenilor. În plus, asigurarea unei administrații publice sigure și reziliente reprezintă o piatră de temelie a transformării digitale a societății în ansamblu.

Prezenta propunere se bazează pe Strategia UE privind uniunea securității [COM(2020) 605 final] și pe Strategia de securitate cibernetică a UE pentru deceniul digital [JOIN(2020) 18 final].

Propunerea modernizează cadrul juridic existent referitor la CERT-UE și ia în considerare evoluția și intensificarea digitalizării instituțiilor, organelor și agențiilor în ultimii ani, precum și evoluția situației amenințărilor la adresa securității cibernetice. Ambele tendințe s-au amplificat de la începutul crizei provocate de pandemia de COVID-19, în timp ce numărul incidentelor continuă să crească, iar atacurile provenind dintr-o gamă largă de surse sunt din ce în ce mai sofisticate.

Propunerea prevede schimbarea denumirii CERT-UE din „Centrul de răspuns la incidente de securitate cibernetică” în „Centrul de securitate cibernetică” pentru instituțiile, organele și agențiile Uniunii, în concordanță cu evoluțiile din statele membre și de la nivel mondial, unde multe astfel de centre și-au schimbat denumirea în centre de securitate cibernetică, urmând să se păstreze denumirea prescurtată „CERT-UE”, deoarece este recunoscută pe scară largă.

• Coerența cu dispozițiile existente în domeniul de politică vizat

Prezenta propunere vizează creșterea rezilienței în materie de securitate cibernetică a instituțiilor, organelor și agențiilor Uniunii împotriva amenințărilor cibernetice, aliniindu-se în același timp la legislația existentă:

- Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune. De asemenea, propunerea se aliniază la propunerea de Directivă (UE) XXXX/XXXX privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/1148 [propunerea de Directivă NIS 2];

- Regulamentul (UE) 2019/881 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor (Regulamentul privind securitatea cibernetică);

- Propunere de Regulament (UE) XXXX/XXXX privind securitatea informațiilor în instituțiile, organele, oficiile și agențiile Uniunii;

- Recomandarea Comisiei din 23 iunie 2021 privind crearea unei unități cibernetice comune;

- Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare;

Anexa la Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare stabilește Planul de acțiune privind răspunsul coordonat la incidentele și crizele de securitate cibernetică transfrontaliere de mare amploare.

În rezoluția din 9 martie 2021, Consiliul Uniunii Europene a subliniat că securitatea cibernetică este vitală pentru funcționarea administrației publice atât la nivel național, cât și la nivelul UE, precum și pentru societate și economie în ansamblu, subliniind importanța unui cadru de securitate solid și coerent pentru protejarea întregului personal, a datelor, a rețelelor de comunicații, a sistemelor informatice și a proceselor decizionale ale UE. În special, acest lucru trebuie realizat prin sporirea rezilienței și îmbunătățirea culturii securității în instituțiile, organele și agențiile Uniunii. Trebuie puse la dispoziție resurse și capacități suficiente, inclusiv în contextul consolidării mandatului CERT-UE.

2. TEMEIUL JURIDIC, SUBSIDIARITATEA ȘI PROPORȚIONALITATEA

- **Temeiul juridic**

Temeiul juridic al prezentului regulament este articolul 298 din Tratatul privind funcționarea Uniunii Europene (TFUE), care prevede că, în îndeplinirea misiunilor lor, instituțiile, organele, oficiile și agențiile Uniunii sunt susținute de o administrație europeană transparentă, eficientă și independentă. În scopul respectării Statutului funcționarilor Uniunii Europene și Regimului aplicabil altor agenți ai Uniunii, adoptate în temeiul articolului 336, Parlamentul European și Consiliul, hotărând prin regulamente, în conformitate cu procedura legislativă ordinară, stabilesc dispozițiile necesare.

Tehnologia informației a oferit instituțiilor, organelor și agențiilor Uniunii noi modalități de a lucra, de a interacționa cu cetățenii și de a-și îmbunătăți operațiunile generale. Peisajul amenințărilor cibernetice evoluează odată cu tehnologia. Instituțiile, organele și agențiile Uniunii au devenit ținte extrem de atractive ale unor atacuri cibernetice sofisticate. Instituirea de sisteme și cerințe pentru asigurarea securității cibernetice pare să contribuie la sporirea eficienței și la asigurarea independenței administrației europene, astfel încât instituțiile, organele, oficiile și agențiile Uniunii să își poată desfășura misiunile într-un mod mai eficient într-o lume digitală.

În plus, disparitățile actuale, astfel cum se explică în secțiunea 3 de mai jos, dintre postura și abordarea în materie de securitate cibernetică a instituțiilor, organelor și agențiilor Uniunii reprezintă alte obstacole în calea unei administrații europene transparente, eficiente și independente. În lipsa unei abordări comune, postura de securitate cibernetică în rândul instituțiilor, organelor și agențiilor Uniunii ar continua să se dezvolte în direcții divergente. Prin urmare, acest temei juridic este adecvat, având în vedere că regulamentul urmărește să creeze un cadru juridic comun pentru securitatea cibernetică în instituțiile, organele, oficiile și agențiile Uniunii.

- **Subsidiaritatea**

Regulamentul privind măsuri pentru un nivel comun ridicat de securitate cibernetică pentru toate instituțiile, organele, oficiile și agențiile Uniunii se încadrează în sfera de competență exclusivă a Uniunii.

- **Proporționalitatea**

Normele propuse în prezentul regulament nu depășesc ceea ce este necesar pentru îndeplinirea obiectivelor specifice în mod satisfăcător. Măsurile avute în vedere vor contribui la atingerea unui nivel comun ridicat de securitate cibernetică fără a depăși ceea ce este necesar pentru atingerea obiectivului, având în vedere riscurile tot mai ridicate cu care se confruntă acestea.

- **Alegerea instrumentului**

Un regulament, care este direct aplicabil, este considerat instrumentul juridic adecvat pentru definirea și raționalizarea obligațiilor impuse instituțiilor, organelor și agențiilor Uniunii. Pentru a permite îmbunătățiri specifice, un regulament este cel mai adecvat instrument juridic.

3. REZULTATELE EVALUĂRILOR EX-ANTE, ALE CONSULTĂRILOR CU PĂRȚILE INTERESATE ȘI ALE EVALUĂRILOR IMPACTULUI

- **Evaluările ex-ante**

CERT-UE a efectuat o evaluare a principalelor amenințări cibernetice la care instituțiile, organele și agențiile Uniunii sunt expuse în prezent sau la care există riscul să fie expuse în viitorul apropiat.

În analiză au fost utilizate trei categorii de observații:

- tentativele de accesare neautorizată a infrastructurii informatice a instituțiilor, organelor și agențiilor Uniunii (atunci când reușesc, acestea sunt tratate ca incidente, iar în celelalte cazuri sunt înregistrate ca tentative detectate);
- amenințările detectate în apropierea instituțiilor, organelor și agențiilor Uniunii (de exemplu, în sectoarele lor conexe, în comunitățile lor de părți interesate sau în Europa);
- tendințe majore ale amenințărilor observate la nivel mondial.

În plus, analiza a examinat modul în care schimbările majore actuale afectează modul în care instituțiile Uniunii își gestionează și își utilizează infrastructura și serviciile informatice. Printre aceste schimbări se numără:

- creșterea volumului de telemuncă;
- migrarea sistemelor către cloud;
- creșterea nivelului de externalizare a serviciilor informatice.

În perioada 2019-2021, numărul incidentelor semnificative[1] care au afectat instituțiile, organele și agențiile Uniunii, provocate de actori care generează amenințări persistente avansate (APT), a crescut dramatic. În prima jumătate a anului 2021, numărul incidentelor semnificative a fost echivalent cu cel înregistrat pe parcursul întregului an 2020. Acest lucru se reflectă, de asemenea, în numărul de copii conforme (instantanee ale conținutului sistemelor sau dispozitivelor afectate) analizate de CERT-UE în 2020, care s-a triplat în comparație cu 2019, în timp ce numărul incidentelor semnificative a crescut de peste zece ori față de 2018.

În 2020, comitetul director al CERT-UE a stabilit un nou obiectiv strategic pentru CERT-UE de a garanta un nivel cuprinzător de apărare cibernetică pentru toate instituțiile, organele și agențiile, cu o amploare și o profunzime adecvată, precum și o adaptare continuă la amenințările actuale sau iminente, inclusiv atacurile împotriva dispozitivelor mobile, a mediilor cloud și a dispozitivelor conectate prin internetul obiectelor.

Pe lângă analiza amenințărilor realizată de CERT-UE, Comisia a efectuat o evaluare a funcționării în materie de securitate cibernetică a 20 de instituții, organe și agenții ale Uniunii. Aceasta a oferit informații cu privire la practicile consacrate în materie de securitate cibernetică și la capacitățile de gestionare a securității cibernetice, cu o analiză comparativă externă a unor controale tehnice de securitate.

Această evaluare s-a bazat pe chestionare la care au răspuns aceste instituții, organe și agenții, pe date aflate la dispoziția publicului și pe date furnizate direct de instituțiile, organele și agențiile Uniunii. Evaluarea oferă suficiente informații cu privire la situația actuală pentru a formula următoarele concluzii:

- maturitatea securității cibernetice, dimensiunea infrastructurii informatice și nivelurile de capabilități variază substanțial în rândul instituțiilor, organelor și agențiilor Uniunii evaluate;

- deși multe instituții, organe și agenții ale Uniunii dispun, în general, de capacități de detectare și de răspuns mature, au fost constatate niveluri diferite de gestionare integrată a riscurilor în ceea ce privește capacitățile lor de guvernanță în domeniul securității cibernetice;

- deși, în general, cadrele de securitate cibernetică (strategie, politică și o bază de norme) ale instituțiilor, organelor și agențiilor Uniunii evaluate sunt bine stabilite în domeniile-cheie de securitate cibernetică enumerate în anexa I la regulament, unele instituții, organe și agenții ale Uniunii nu dispun de capacități mature de gestionare a continuității activității, de asigurare a conformității, de audit și de îmbunătățire continuă;

- s-a constatat că instituțiile, organele și agențiile Uniunii incluse în evaluare aplică în mod inegal măsurile tehnice considerate cele mai bune practici.

Pe scurt, analiza celor 20 de instituții, organe și agenții ale Uniunii indică faptul că guvernanța, igiena cibernetică, capacitatea generală și maturitatea acestora variază pe un spectru larg. Prin urmare, este esențial ca toate instituțiile, organele și agențiile Uniunii să

[1] „Incident semnificativ” înseamnă orice incident, cu excepția cazului în care acesta are un impact limitat și este probabil ca metoda sau tehnologia sa să fie deja bine înțeleasă.

pună în aplicare un nivel de referință al măsurilor de securitate cibernetică, pentru a aborda această disparitate în ceea ce privește maturitatea și pentru a asigura un nivel comun ridicat de securitate cibernetică pentru toate instituțiile, organele și agențiile Uniunii.

Până în prezent, niciun act legislativ al Uniunii nu s-a axat pe securitatea cibernetică a instituțiilor, organelor și agențiilor Uniunii și nu a abordat în mod cuprinzător peisajul amenințărilor la adresa securității cibernetice și riscurile informatice emergente generate de digitalizare.

- **Consultările cu părțile interesate**

Comisia a consultat părțile interesate din cadrul instituțiilor, organelor și agențiilor Uniunii, precum și reprezentanții statelor membre în cadrul Consiliului și părțile interesate din Parlamentul European. La 25 iunie 2021, reprezentanți ai statelor membre și ai părților interesate relevante din instituțiile, organele și agențiile Uniunii au participat la un atelier organizat de Comisie pentru a discuta cu privire la conținutul viitoarei propuneri de regulament.

- **Evaluarea impactului**

Prezenta propunere va avea un impact asupra instituțiilor, organelor și agențiilor Uniunii. Prin urmare, nu este necesară o evaluare specifică a impactului, deoarece nu se va aplica statelor membre.

- **Drepturile fundamentale**

Uniunea Europeană se angajează să asigure standarde înalte de protecție a drepturilor fundamentale. Toate schimburile de informații în temeiul prezentului regulament ar urma să se desfășoare în medii de încredere, cu respectarea deplină a dreptului la protecția datelor cu caracter personal, astfel cum este prevăzut la articolul 8 din Carta drepturilor fundamentale a Uniunii Europene, și a legislației relevante privind protecția datelor, în special a Regulamentului (UE) 2018/1725 al Parlamentului European și al Consiliului.

4. IMPLICAȚII BUGETARE

Potrivit analizelor comparative și studiilor de piață[2], cheltuielile directe în domeniul securității cibernetice au avut tendința de a varia între 4 și 7 % din cheltuielile agregate în domeniul tehnologiei informației ale organizațiilor. Cu toate acestea, analiza amenințărilor efectuată de CERT-UE în sprijinul prezentei propuneri legislative indică faptul că organismele internaționale și organizațiile politice se confruntă cu riscuri sporite și, prin urmare, un nivel de 10 % din cheltuielile în domeniul tehnologiei informației alocate pentru securitatea cibernetică ar părea un obiectiv mai adecvat. Costul exact al acestor eforturi nu poate fi determinat din cauza lipsei de informații detaliate privind cheltuielile în domeniul tehnologiei

[2] Sursa: Gartner, „Identifying the Real Information Security Budget” (Identificarea bugetului real pentru securitatea informațiilor) (2016). Acesta se adaugă cheltuielilor indirecte legate de securitatea sistemelor informatice, cum ar fi cheltuielile pentru securitatea rețelelor, și anume firewall-uri, programe antivirus și responsabilitățile proprietarilor de sisteme, precum evaluarea riscurilor și punerea în aplicare a controalelor de securitate. Conform unui document din 2020, cheltuielile legate de securitatea cibernetică ale instituțiilor financiare reprezintă 10-11 % din cheltuielile în domeniul tehnologiei informației, sursa: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

informației ale instituțiilor, organelor și agențiilor Uniunii și ponderea relevantă a cheltuielilor legate de securitatea cibernetică.

Prin urmare, deși este probabil ca multe instituții, organe și agenții ale Uniunii să cheltuiască pentru securitatea cibernetică mai puțin decât ar trebui de fapt, prezentul regulament nu va determina, ca atare, o creștere a cheltuielilor curente respective. Chiar și în absența regulamentului, fiecare entitate ar fi nevoită să asigure un nivel adecvat de securitate cibernetică. Regulamentul continuă cooperarea anterioară din cadrul Comitetului director al CERT-UE și oficializează un nivel de schimb de informații deja parțial existent. După cum se detaliază în fișa financiară legislativă, CERT-UE va avea nevoie de resurse suplimentare pentru a-și îndeplini rolul extins, iar aceste resurse trebuie să fie realocate de la instituțiile, organele și agențiile Uniunii care beneficiază de serviciile CERT-UE.

5. ALTE ELEMENTE

- **Măsuri de punere în aplicare, de monitorizare, de evaluare și de raportare**

Consiliul interinstituțional pentru securitate cibernetică (IICB), cu sprijinul CERT-UE, trebuie să revizuiască funcționarea prezentului regulament, să efectueze evaluări și să prezinte Comisiei un raport cuprinzând constatările sale. Comisia trebuie să asigure că se transmit periodic rapoarte Parlamentului European, Consiliului, Comitetului Economic și Social European și Comitetului Regiunilor.

CERT-UE poate elabora o propunere de document de orientare sau de recomandare, pe care IICB poate alege să o adopte. Un document de orientare este un document consultativ care se adresează tuturor sau unei părți dintre instituțiile, organele și agențiile Uniunii, în timp ce o recomandare se adresează instituțiilor, organelor și agențiilor individuale ale Uniunii. Un apel la acțiune este un document consultativ al CERT-UE care descrie măsurile urgente de securitate pe care instituțiile, organele și agențiile Uniunii sunt invitate să le adopte într-un termen stabilit.

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

<u>Dispoziții generale</u>

Regulamentul stabilește măsuri în vederea asigurării unui nivel comun ridicat de securitate cibernetică și se aplică instituțiilor, organelor și agențiilor Uniunii pentru a le permite să își îndeplinească misiunile într-un mod transparent, eficient și independent. (Articolele 1-3 și 23-25)

<u>Măsuri pentru un nivel comun ridicat de securitate cibernetică</u>

Instituțiile, organele și agențiile Uniunii sunt obligate să instituie un cadru intern de gestionare, guvernanță și control al riscurilor în materie de securitate cibernetică, care să asigure o gestionare eficace și prudentă a tuturor riscurilor de securitate cibernetică. În plus, instituțiile, organele și agențiile adoptă un nivel de referință în materie de securitate cibernetică pentru a aborda riscurile identificate în cadrul respectiv, pentru a evalua periodic maturitatea în materie de securitate cibernetică și pentru a adopta un plan de securitate cibernetică. (Articolele 4-8)

<u>Consiliul interinstituțional pentru securitate cibernetică</u>

Se instituie Consiliul interinstituțional pentru securitate cibernetică, responsabil pentru monitorizarea punerii în aplicare a prezentului regulament de către instituțiile, organele și agențiile Uniunii, precum și pentru supravegherea punerii în aplicare de către CERT-UE a priorităților și obiectivelor generale și pentru elaborarea de orientări strategice pentru CERT-UE. (Articolele 9-11)

CERT-UE

CERT-UE contribuie la securitatea mediului informatic al tuturor instituțiilor, organelor și agențiilor Uniunii, oferindu-le consiliere, contribuind la prevenirea, detectarea, atenuarea și răspunsul la incidente și acționând ca centru de schimb de informații în materie de securitate cibernetică și de coordonare a răspunsului la incidente pentru aceste entități. (Articolele 12-17)

Obligații de cooperare și de raportare

Regulamentul asigură cooperarea și schimbul de informații între CERT-UE și instituțiile, organele și agențiile Uniunii pentru a consolida încrederea. În acest scop, CERT-UE poate solicita instituțiilor, organelor și agențiilor Uniunii să îi furnizeze informații relevante, poate face schimb de informații referitoare la incidente cu instituțiile, organele și agențiile Uniunii pentru a facilita detectarea amenințărilor sau incidentelor cibernetice similare fără consimțământul entității afectate. CERT-UE poate face schimb de informații referitoare la incidente care dezvăluie identitatea persoanei vizate de incidentul de securitate cibernetică numai cu consimțământul entității afectate.

În special, toate instituțiile, organele și agențiile Uniunii notifică CERT-UE cu privire la amenințările cibernetice semnificative, vulnerabilitățile semnificative și incidentele semnificative, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la data la care au luat cunoștință de acestea. (Articolele 18-22)

2022/0085 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 298,

având în vedere Tratatul de instituire a Comunității Europene a Energiei Atomice, în special articolul 106a,

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) În era digitală, tehnologia informației și comunicațiilor este o piatră de temelie a unei administrații transparente, eficiente și independente a Uniunii. Evoluția tehnologiei și creșterea gradului de complexitate și de interconectare a sistemelor digitale amplifică riscurile de securitate cibernetică, făcând administrația Uniunii mai vulnerabilă la amenințările și incidentele cibernetice, care reprezintă, în cele din urmă, amenințări la adresa continuității activității administrației și a capacității acesteia de a-și proteja datele. Deși utilizarea sporită a serviciilor de tip cloud computing, utilizarea ubicuă a tehnologiei informației, nivelul ridicat de digitalizare, munca la distanță și evoluția tehnologiei și a conectivității sunt, în prezent, caracteristici esențiale ale tuturor activităților entităților administrative ale Uniunii, reziliența digitală nu este încă suficient integrată.

(2) Peisajul amenințărilor cibernetice cu care se confruntă instituțiile, organele și agențiile Uniunii este într-o continuă evoluție. Tacticile, tehnicile și procedurile utilizate de actorii care generează amenințări sunt într-o continuă evoluție, în timp ce principalele motive ale acestor atacuri se schimbă foarte puțin, de la furtul de informații confidențiale valoroase până la sustragerea de bani, manipularea opiniei publice sau subminarea infrastructurii digitale. Ritmul în care își desfășoară atacurile cibernetice continuă să crească, în timp ce campaniile lor sunt din ce în ce mai sofisticate și automatizate, vizând suprafețe de atac expuse care continuă să se extindă și exploatând rapid vulnerabilitățile.

(3) Mediile informatice ale instituțiilor, organelor și agențiilor Uniunii au interdependențe și fluxuri de date integrate, iar utilizatorii acestora colaborează îndeaproape. Această

interconectare înseamnă că orice perturbare, chiar și atunci când este limitată inițial la o instituție, un organ sau o agenție a Uniunii, poate avea efecte în cascadă în sens mai larg, ceea ce ar putea avea impacturi negative de amploare și de lungă durată asupra celorlalte. În plus, mediile informatice ale anumitor instituții, organe și agenții sunt conectate cu cele ale statelor membre, ceea ce face ca un incident în cadrul unei entități a Uniunii să reprezinte un risc de securitate cibernetică a mediilor informatice ale statelor membre și viceversa.

(4) Instituțiile, organele și agențiile Uniunii sunt ținte atractive, care se confruntă cu actori care generează amenințări cu înaltă calificare și care dispun de resurse suficiente, precum și cu alte amenințări. În același timp, nivelul și maturitatea rezilienței cibernetice și capacitatea de a detecta și de a răspunde activităților cibernetice răuvoitoare variază semnificativ între aceste entități. Prin urmare, pentru buna funcționare a administrației europene este necesar ca instituțiile, organele și agențiile Uniunii să atingă un nivel comun ridicat de securitate cibernetică printr-un „nivel de referință în materie de securitate cibernetică” (un set de norme minime în materie de securitate cibernetică pe care rețelele și sistemele informatice, precum și operatorii și utilizatorii acestora trebuie să le respecte pentru a reduce la minimum riscurile de securitate cibernetică), prin schimbul de informații și colaborarea în acest domeniu.

(5) [Propunerea de Directivă NIS 2] privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune urmărește să îmbunătățească și mai mult capacitatea de reziliență și capacitatea de răspuns la incidente ale entităților publice și private, ale autorităților și organelor naționale competente, precum și ale Uniunii în ansamblu. Prin urmare, este necesar ca instituțiile, organele și agențiile Uniunii să urmeze exemplul prin asigurarea unor norme care să fie coerente cu [propunerea de Directivă NIS 2] și să reflecte nivelul său de ambiție.

(6) Pentru a atinge un nivel comun ridicat de securitate cibernetică, este necesar ca fiecare instituție, organ sau agenție a Uniunii să instituie un cadru intern de gestionare, guvernanță și control al riscurilor de securitate cibernetică, care să asigure o gestionare eficace și prudentă a tuturor riscurilor de securitate cibernetică și să țină seama de gestionarea continuității activității și de gestionarea crizelor.

(7) Diferențele dintre instituțiile, organele și agențiile Uniunii necesită o anumită flexibilitate în ceea ce privește punerea în aplicare, deoarece nu există o abordare universală. Măsurile pentru un nivel comun ridicat de securitate cibernetică nu ar trebui să includă nicio obligație care să interfereze în mod direct cu exercitarea misiunilor instituțiilor, organelor și agențiilor Uniunii sau să aducă atingere autonomiei lor instituționale. Astfel, aceste instituții, organe și agenții trebuie să își stabilească propriile cadre pentru gestionarea, guvernanța și controlul riscurilor de securitate cibernetică și să adopte propriile planuri de referință și de securitate cibernetică.

(8) Pentru a evita impunerea unei sarcini financiare și administrative disproporționate asupra instituțiilor, organelor și agențiilor Uniunii, cerințele de gestionare a riscurilor de securitate cibernetică trebuie să fie proporționale cu riscurile la care sunt expuse rețeaua și sistemul informatic în cauză, ținându-se seama de cea mai avansată tehnologie corespunzătoare unor astfel de măsuri. Fiecare instituție, organ sau agenție a Uniunii trebuie să urmărească alocarea unui procent adecvat din bugetul său în domeniul tehnologiei informației pentru a-și îmbunătăți nivelul de securitate

cibernetică; pe termen lung, ar trebui să se urmărească atingerea unui obiectiv de 10 %.

(9) Pentru asigurarea unui nivel comun ridicat de securitate cibernetică, aceasta trebuie să se afle sub supravegherea celui mai înalt nivel de conducere al fiecărei instituții, agenții și al fiecărui organ al Uniunii, care trebuie să aprobe un nivel de referință în materie de securitate cibernetică, care să abordeze riscurile identificate în cadrul stabilit de fiecare instituție, organ și agenție. Abordarea culturii securității cibernetice, adică practica zilnică în domeniul securității cibernetice, este parte integrantă a unui nivel de referință în materie de securitate cibernetică în toate instituțiile, organele și agențiile Uniunii.

(10) Instituțiile, organele și agențiile Uniunii trebuie să evalueze riscurile legate de relațiile cu furnizorii și prestatorii de servicii, inclusiv cu prestatorii de servicii de stocare și prelucrare a datelor sau de servicii de securitate gestionate, și să ia măsurile adecvate pentru a combate astfel de riscuri. Aceste măsuri trebuie să facă parte din nivelul de referință în materie de securitate cibernetică și să fie detaliate în documentele de orientare sau în recomandările emise de CERT-UE. La definirea măsurilor și a orientărilor trebuie să se țină seama în mod corespunzător de legislația și politicile relevante ale UE, inclusiv de evaluările riscurilor și de recomandările emise de Grupul de cooperare privind securitatea rețelelor și a informațiilor, cum ar fi evaluarea coordonată la nivelul UE a riscurilor de securitate cibernetică aferente rețelelor 5G și setul de instrumente al UE privind securitatea cibernetică a rețelelor 5G. În plus, ar putea fi necesară certificarea produselor, a serviciilor și a proceselor TIC relevante, în cadrul sistemelor europene specifice de certificare a securității cibernetice adoptate în temeiul articolului 49 din Regulamentul (UE) 2019/881.

(11) În mai 2011, secretarii generali ai instituțiilor și organelor Uniunii au decis să constituie o echipă de preconfigurare a unui centru de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile Uniunii (CERT-UE), supervizată de un comitet director interinstituțional. În iulie 2012, secretarii generali au confirmat modalitățile practice și au convenit să mențină CERT-UE ca entitate permanentă, pentru a contribui în continuare la îmbunătățirea nivelului general de securitate a tehnologiei informației la nivelul instituțiilor, organelor și agențiilor Uniunii, ca exemplu de cooperare interinstituțională vizibilă în domeniul securității cibernetice. În septembrie 2012, CERT-UE a fost înființat ca grup operativ al Comisiei Europene, cu un mandat interinstituțional. În decembrie 2017, instituțiile și organele Uniunii au încheiat un acord interinstituțional privind organizarea și funcționarea CERT-UE[3]. Acest mecanism ar trebui să evolueze în continuare pentru a sprijini punerea în aplicare a prezentului regulament.

(12) Denumirea CERT-UE trebuie schimbată din „Centrul de răspuns la incidente de securitate cibernetică” în „Centrul de securitate cibernetică” pentru instituțiile, organele și agențiile Uniunii, în concordanță cu evoluțiile din statele membre și de la nivel mondial, unde multe astfel de centre și-au schimbat denumirea în centre de securitate cibernetică, însă trebuie păstrată denumirea prescurtată „CERT-UE”, deoarece este recunoscută pe scară largă.

[3] JO C 12, 13.1.2018, p. 1.

(13) Multe atacuri cibernetice fac parte din campanii mai ample care vizează grupuri de instituții, organe și agenții ale Uniunii sau comunități de interes care includ instituții, organe și agenții ale Uniunii. Pentru a permite detectarea proactivă, răspunsul la incidente sau măsurile de atenuare, instituțiile, organele și agențiile Uniunii trebuie să informeze CERT-UE cu privire la amenințările cibernetice semnificative, vulnerabilitățile semnificative și incidentele semnificative și să facă schimb de detalii tehnice adecvate care să permită detectarea sau atenuarea amenințărilor cibernetice, a vulnerabilităților și a incidentelor similare în alte instituții, organe și agenții ale Uniunii, precum și răspunsul la astfel de amenințări, vulnerabilități și incidente. Urmând aceeași abordare precum cea prevăzută în [propunerea de Directivă NIS 2], în cazul în care iau cunoștință de un incident semnificativ, entitățile trebuie să transmită CERT-UE o notificare inițială în termen de 24 de ore. Acest schimb de informații trebuie să permită CERT-UE să disemineze informațiile către alte instituții, organe și agenții ale Uniunii, precum și către omologii corespunzători, pentru a contribui la protejarea mediilor informatice ale Uniunii și ale omologilor Uniunii împotriva unor incidente, amenințări și vulnerabilități similare.

(14) Pe lângă atribuirea mai multor sarcini și a unui rol extins pentru CERT-UE, este necesară instituirea unui Consiliu interinstituțional pentru securitate cibernetică (IICB), care să faciliteze un nivel comun ridicat de securitate cibernetică în rândul instituțiilor, organelor și agențiilor Uniunii prin monitorizarea punerii în aplicare a prezentului regulament de către instituțiile, organele și agențiile Uniunii, prin supravegherea punerii în aplicare a priorităților și a obiectivelor generale de către CERT-UE și prin elaborarea unor orientări strategice pentru CERT-UE. IICB trebuie să asigure reprezentarea instituțiilor și să includă reprezentanți ai agențiilor și ai organelor prin intermediul Rețelei agențiilor UE.

(15) CERT-UE trebuie să sprijine punerea în aplicare a măsurilor pentru un nivel comun ridicat de securitate cibernetică prin propuneri de documente de orientare și recomandări adresate IICB sau prin adresarea unor apeluri la acțiune. Astfel de documente de orientare și recomandări trebuie să fie aprobate de IICB. Atunci când este necesar, CERT-UE trebuie să adreseze apeluri la acțiune care să descrie măsurile urgente de securitate pe care instituțiile, organele și agențiile Uniunii sunt îndemnate să le adopte într-un termen stabilit.

(16) IICB trebuie să monitorizeze respectarea regulamentului, precum și punerea în aplicare a documentelor de orientare, a recomandărilor și a apelurilor la acțiune adresate de CERT-UE. În ceea ce privește aspectele tehnice, IICB trebuie să beneficieze de sprijin din partea grupurilor consultative tehnice a căror componență este decisă de IICB, care ar trebui să lucreze în strânsă cooperare cu CERT-UE, cu instituțiile, organele și agențiile Uniunii și cu alte părți interesate, după caz. Dacă este necesar, IICB trebuie să emită avertismente fără caracter obligatoriu și să recomande audituri.

(17) CERT-UE trebuie să aibă misiunea de a contribui la securitatea mediului informatic al tuturor instituțiilor, organelor și agențiilor Uniunii. CERT-UE trebuie să acționeze ca echivalent al coordonatorului desemnat pentru instituțiile, organele și agențiile Uniunii, în scopul divulgării coordonate a vulnerabilităților către registrul european al vulnerabilităților, astfel cum se menționează la articolul 6 din [propunerea de Directivă NIS 2].

(18) În 2020, comitetul director al CERT-UE a stabilit un nou obiectiv strategic pentru CERT-UE de a garanta un nivel cuprinzător de apărare cibernetică pentru toate instituțiile, organele și agențiile Uniunii, cu o amploare și o profunzime adecvate, precum și o adaptare continuă la amenințările actuale sau iminente, inclusiv atacurile împotriva dispozitivelor mobile, a mediilor cloud și a dispozitivelor conectate prin internetul obiectelor. Acest obiectiv strategic include, de asemenea, centre de operațiuni pentru securitate (SOC) cu spectru larg, care monitorizează rețelele, precum și monitorizarea permanentă a amenințărilor deosebit de grave. CERT-UE trebuie să ofere sprijin echipelor de securitate informatică ale instituțiilor, organelor și agențiilor mai mari ale Uniunii, inclusiv prin monitorizarea non-stop din prima linie. Pentru instituțiile, organele și agențiile mai mici și unele medii ale Uniunii, CERT-UE trebuie să furnizeze toată gama de servicii.

(19) De asemenea, CERT-UE trebuie să își îndeplinească rolul prevăzut în [propunerea de Directivă NIS 2] privind cooperarea și schimbul de informații cu rețeaua echipelor de intervenție în caz de incidente de securitate informatică (CSIRT). În plus, în conformitate cu Recomandarea (UE) 2017/1584 a Comisiei[4], CERT-UE trebuie să coopereze cu părțile interesate relevante pentru a identifica un răspuns coordonat. Pentru a contribui la un nivel ridicat de securitate cibernetică în întreaga Uniune, CERT-UE trebuie să facă schimb de informații referitoare la incidente cu omologii naționali. CERT-UE trebuie, de asemenea, să colaboreze cu alți omologi din sectorul public și privat, inclusiv din cadrul NATO, sub rezerva aprobării prealabile de către IICB.

(20) În sprijinirea cooperării operaționale în domeniul securității cibernetice, CERT-UE trebuie să utilizeze expertiza de care dispune Agenția Uniunii Europene pentru Securitate Cibernetică prin intermediul unei cooperări structurate, astfel cum se prevede în Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[5]. Dacă este cazul, între cele două entități ar trebui încheiate acorduri specifice pentru a se stabili modalitățile practice de punere în aplicare a acestei cooperări și pentru a se evita suprapunerea activităților. CERT-UE trebuie să coopereze cu Agenția Uniunii Europene pentru Securitate Cibernetică în ceea ce privește analiza amenințărilor și să transmită agenției în mod regulat raportul său privind situația amenințărilor.

(21) În sprijinul unității cibernetice comune, create în conformitate cu Recomandarea Comisiei din 23 iunie 2021[6], este necesar ca CERT-UE să coopereze și să facă schimb de informații cu părțile interesate pentru a încuraja cooperarea operațională și pentru a permite rețelelor existente să își valorifice pe deplin potențialul de protejare a Uniunii.

---

4 Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare (JO L 239, 19.9.2017, p. 36).

5 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).

6 Recomandarea Comisiei C(2021) 4520 din 23.6.2021 privind crearea unei unități cibernetice comune.

(22) Toate datele cu caracter personal prelucrate în temeiul prezentului regulament trebuie prelucrate în conformitate cu legislația privind protecția datelor, inclusiv cu Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului[7].

(23) CERT-UE și instituțiile, organele și agențiile Uniunii trebuie să gestioneze informațiile în conformitate cu normele prevăzute în regulament [propunerea de regulament privind securitatea informațiilor]. Pentru a asigura coordonarea în materie de securitate, orice contacte cu CERT-UE inițiate sau solicitate de serviciile naționale de securitate și de informații trebuie comunicate fără întârzieri nejustificate Direcției Securitate a Comisiei și președintelui IICB.

(24) Întrucât serviciile și sarcinile CERT-UE sunt în interesul tuturor instituțiilor, organelor și agențiilor Uniunii, fiecare instituție, organ și agenție a Uniunii cu cheltuieli în domeniul tehnologiei informației trebuie să contribuie în mod echitabil la aceste servicii și sarcini. Contribuțiile respective nu aduc atingere autonomiei bugetare a instituțiilor, organelor și agențiilor Uniunii.

(25) IICB, cu sprijinul CERT-UE, trebuie să revizuiască și să evalueze punerea în aplicare a prezentului regulament și trebuie să raporteze constatările sale Comisiei. Pe baza acestui input, Comisiei îi revine sarcina de a transmite rapoarte Parlamentului European, Consiliului, Comitetului Economic și Social European și Comitetului Regiunilor.

ADOPTĂ PREZENTUL REGULAMENT:

Capitolul I
DISPOZIȚII GENERALE

Articolul 1
Obiect

Prezentul regulament stabilește:

(a) obligații pentru instituțiile, organele și agențiile Uniunii de a institui un cadru intern de gestionare, guvernanță și control al riscurilor de securitate cibernetică;

(b) obligații de gestionare a riscurilor de securitate cibernetică și de raportare pentru instituțiile, organele și agențiile Uniunii

(c) norme privind organizarea și funcționarea Centrului de securitate cibernetică pentru instituțiile, organele și agențiile Uniunii (CERT-UE) și privind organizarea și funcționarea Consiliului interinstituțional pentru securitate cibernetică (IICB).

[7] 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).

Articolul 2
Domeniul de aplicare

Prezentul regulament se aplică gestionării, guvernanței și controlului riscurilor de securitate cibernetică de către toate instituțiile, organele și agențiile Uniunii, precum și organizării și funcționării CERT-UE și a Consiliului interinstituțional pentru securitate cibernetică.

Articolul 3
Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

(1) „instituții, organe și agenții ale Uniunii” înseamnă instituțiile, organele și agențiile Uniunii înființate prin Tratatul privind Uniunea Europeană, Tratatul privind funcționarea Uniunii Europene sau Tratatul de instituire a Comunității Europene a Energiei Atomice sau în temeiul acestora;

(2) „rețea și sistem informatic” înseamnă rețea și sistem informatic în sensul articolului 4 punctul 1 din [propunerea de Directivă NIS 2];

(3) „securitatea rețelelor și a sistemelor informatice” înseamnă securitatea rețelelor și a sistemelor informatice în sensul articolului 4 punctul 2 din [propunerea de Directivă NIS 2];

(4) „securitate cibernetică” înseamnă securitatea cibernetică în sensul articolului 4 punctul 3 din [propunerea de Directivă NIS 2];

(5) „cel mai înalt nivel de conducere” înseamnă un manager, un organ de conducere sau de coordonare și supraveghere de la cel mai înalt nivel administrativ, ținând seama de mecanismele de guvernanță la nivel înalt din fiecare instituție, organ sau agenție a Uniunii;

(6) „incident” înseamnă incident în sensul articolului 4 punctul 5 din [propunerea de Directivă NIS 2];

(7) „incident semnificativ” înseamnă orice incident, cu excepția cazului în care acesta are un impact limitat și este probabil ca metoda sau tehnologia sa să fie deja bine înțeleasă;

(8) „atac major” înseamnă orice incident care necesită mai multe resurse decât cele disponibile la instituția, organul sau agenția Uniunii afectată și la CERT-UE;

(9) „administrarea incidentelor” înseamnă administrarea incidentelor în sensul articolului 4 punctul 6 din [propunerea de Directivă NIS 2];

(10) „amenințare cibernetică” înseamnă o amenințare cibernetică în sensul articolului 2 punctul 8 din Regulamentul (UE) 2019/881;

(11) „amenințare cibernetică semnificativă” înseamnă o amenințare cibernetică cu intenția, oportunitatea și capacitatea de a cauza un incident semnificativ;

(12) „vulnerabilitate” înseamnă vulnerabilitate în sensul articolului 4 punctul 8 din Directiva [propunerea NIS 2];

(13) „vulnerabilitate semnificativă” înseamnă o vulnerabilitate care prezintă riscul de a cauza un incident semnificativ dacă este exploatată;

(14) „risc de securitate cibernetică” înseamnă orice circumstanță sau eveniment ce poate fi identificat în mod rezonabil care are un efect potențial negativ asupra securității rețelelor și a sistemelor informatice;

(15) „unitate cibernetică comună” înseamnă o platformă virtuală și fizică de cooperare pentru diferitele comunități de securitate cibernetică din Uniune, cu accent pe coordonarea operațională și tehnică împotriva amenințărilor și incidentelor cibernetice transfrontaliere majore în sensul Recomandării Comisiei din 23 iunie 2021;

(16) „nivel de referință în materie de securitate cibernetică” înseamnă un set de norme minime în materie de securitate cibernetică pe care rețelele și sistemele informatice, precum și operatorii și utilizatorii acestora trebuie să le respecte, pentru a reduce la minimum riscurile de securitate cibernetică.

Capitolul II
MĂSURI PENTRU UN NIVEL COMUN RIDICAT DE SECURITATE CIBERNETICĂ

Articolul 4
Gestionarea, guvernanța și controlul riscurilor

1. Fiecare instituție, organ și agenție a Uniunii își stabilește propriul cadru intern de gestionare, guvernanță și control al riscurilor de securitate cibernetică (denumit în continuare „cadrul”) pentru a sprijini misiunea entității și pentru a-și exercita autonomia instituțională. Această activitate este supravegheată de cel mai înalt nivel de conducere al entității pentru a se putea asigura o gestionare eficace și prudentă a tuturor riscurilor de securitate cibernetică. Cadrul se instituie până cel târziu la …. [15 luni de la intrarea în vigoare a prezentului regulament].

2. Cadrul acoperă întregul mediu informatic al instituției, organului sau agenției în cauză, inclusiv orice mediu informatic de la fața locului, active și servicii externalizate în medii de cloud computing sau găzduite de părți terțe, dispozitive mobile, rețele corporative, rețele organizaționale care nu sunt conectate la internet și orice dispozitive conectate la mediul informatic. Cadrul ține seama de gestionarea continuității activității și de gestionarea crizelor și ia în considerare securitatea lanțului de aprovizionare, precum și gestionarea riscurilor umane care ar putea avea un impact asupra securității cibernetice a instituției, organului sau agenției Uniunii în cauză.

3. Cel mai înalt nivel de conducere din fiecare instituție, organ și agenție a Uniunii asigură supravegherea respectării de către propria organizație a obligațiilor legate de gestionarea, guvernanța și controlul riscurilor de securitate cibernetică, fără a aduce

atingere responsabilităților formale ale altor niveluri de conducere în ceea ce privește conformitatea și gestionarea riscurilor în domeniile lor respective de responsabilitate.

4. Fiecare instituție, organ și agenție a Uniunii dispune de mecanisme eficace pentru a se asigura că un procent adecvat din bugetul în domeniul tehnologiei informației este cheltuit pentru securitatea cibernetică.

5. Fiecare instituție, organ și agenție a Uniunii numește un responsabil local cu securitatea cibernetică sau o funcție echivalentă care acționează ca punct unic de contact în ceea ce privește toate aspectele securității cibernetice.

Articolul 5
Nivelul de referință în materie de securitate cibernetică

1. Cel mai înalt nivel de conducere din fiecare instituție, organ și agenție a Uniunii își aprobă propriul nivel de referință în materie de securitate cibernetică pentru a aborda riscurile identificate în cadrul menționat la articolul 4 punctul 1. Acest nivel este stabilit în sprijinul misiunii sale și cu exercitarea autonomiei sale instituționale. Nivelul de referință în materie de securitate cibernetică se instituie până cel târziu la …. [18 luni de la intrarea în vigoare a prezentului regulament] și abordează domeniile enumerate în anexa I și măsurile enumerate în anexa II.

2. Personalul de conducere de nivel superior din fiecare instituție, organ și agenție a Uniunii urmează periodic cursuri de formare specifice, pentru a dobândi cunoștințe și competențe suficiente care să le permită să înțeleagă și să evalueze practicile de gestionare a riscurilor de securitate cibernetică, precum și impactul acestora asupra operațiunilor organizației.

Articolul 6
Evaluări ale maturității

Fiecare instituție, organ și agenție a Uniunii efectuează o evaluare a nivelului de maturitate al securității cibernetice cel puțin o dată la trei ani, încorporând toate elementele mediului său informatic, astfel cum este descris la articolul 4, ținând seama de documentele de orientare și de recomandările relevante adoptate în temeiul articolului 13.

Articolul 7
Planuri de securitate cibernetică

1. În urma concluziilor desprinse din evaluarea nivelului de maturitate și luând în considerare activele și riscurile identificate în temeiul articolului 4, cel mai înalt nivel de conducere din fiecare instituție, organ și agenție a Uniunii aprobă un plan de securitate cibernetică, fără întârzieri nejustificate, după instituirea cadrului de gestionare, guvernanță și control al riscurilor și a nivelului de referință în materie de securitate cibernetică. Planul vizează creșterea gradului de securitate cibernetică în ansamblu a entității în cauză și contribuie, astfel, la atingerea sau îmbunătățirea unui nivel comun ridicat de securitate cibernetică în toate instituțiile, organele și agențiile Uniunii. Pentru a sprijini misiunea entității pe baza autonomiei sale instituționale, planul include cel puțin domeniile enumerate în anexa I, măsurile enumerate în anexa

II, precum și măsuri legate de pregătirea pentru incidente, răspunsul la incidente și redresarea în urma incidentelor, cum ar fi monitorizarea și jurnalizarea evenimentelor de securitate. Planul se revizuiește cel puțin o dată la trei ani, în urma evaluărilor nivelului de maturitate, efectuate în temeiul articolului 6.

2. Planul de securitate cibernetică include rolurile și responsabilitățile ce revin membrilor personalului în legătură cu implementarea acestui plan.

3. Planul de securitate cibernetică ia în considerare orice document de orientare și orice recomandare aplicabilă adoptată de CERT-UE.

Articolul 8
Punerea în aplicare

1. După finalizarea evaluărilor nivelului de maturitate, instituțiile, organele și agențiile Uniunii le prezintă Consiliului interinstituțional pentru securitate cibernetică. După ce își finalizează planurile de securitate, instituțiile, organele și agențiile Uniunii informează Consiliul interinstituțional pentru securitate cibernetică în acest sens. La cererea consiliului, ele raportează cu privire la aspecte specifice din prezentul capitol.

2. Documentele de orientare și recomandările emise în temeiul articolului 13 sprijină punerea în aplicare a dispozițiilor prevăzute în prezentul capitol.

Capitolul III
CONSILIUL INTERINSTITUȚIONAL PENTRU SECURITATE CIBERNETICĂ

Articolul 9
Consiliul interinstituțional pentru securitate cibernetică

1. Se instituie Consiliul interinstituțional pentru securitate cibernetică (IICB).

2. IICB este responsabil cu:

   (a) monitorizarea punerii în aplicare a prezentului regulament de către instituțiile, organele și agențiile Uniunii;

   (b) supravegherea punerii în aplicare a priorităților și obiectivelor generale de către CERT-UE și de elaborarea de orientări strategice pentru CERT-UE.

3. IICB este format din trei reprezentanți numiți de Rețeaua agențiilor UE (EUAN), la propunerea Comitetului său consultativ pentru tehnologia informației și comunicațiilor, pentru a reprezenta interesele agențiilor și organelor care își gestionează propriul mediu informatic și câte un reprezentant numit de fiecare dintre următoarele entități:

   (a) Parlamentul European;

   (b) Consiliul Uniunii Europene;

(c) Comisia Europeană;

(d) Curtea de Justiție a Uniunii Europene;

(e) Banca Centrală Europeană;

(f) Curtea de Conturi Europeană;

(g) Serviciul European de Acțiune Externă;

(h) Comitetul Economic Și Social European;

(i) Comitetul European al Regiunilor;

(j) Banca Europeană de Investiții;

(k) Agenția Uniunii Europene pentru Securitate Cibernetică.

Membrii pot fi asistați de un supleant. Alți reprezentanți ai organizațiilor enumerate mai sus sau ai altor instituții, organe și agenții ale Uniunii pot fi invitați de președinte să participe la reuniunile IICB, fără drept de vot.

4. IICB își stabilește regulamentul intern de procedură.

5. IICB numește un președinte din rândul membrilor săi, în conformitate cu regulamentul intern de procedură, pentru o perioadă de patru ani. Supleantul acestuia devine membru titular al IICB pentru aceeași durată.

6. IICB se reunește la inițiativa președintelui, la cererea CERT-UE sau a oricăruia dintre membrii săi.

7. Fiecare membru al IICB dispune de un vot. Deciziile IICB sunt adoptate cu majoritate simplă, cu excepția cazurilor în care se prevede altfel în prezentul regulament. Președintele votează numai în caz de egalitate de voturi, situație în care poate exprima un vot decisiv.

8. IICB poate acționa printr-o procedură scrisă simplificată inițiată în conformitate cu regulamentul intern de procedură. În temeiul procedurii respective, decizia relevantă se consideră aprobată în termenul stabilit de președinte, cu excepția cazului în care un membru formulează obiecții.

9. Șeful CERT-UE sau supleantul acestuia participă la reuniunile IICB, cu excepția cazului în care IICB decide altfel.

10. Secretariatul IICB este asigurat de Comisie.

11. Reprezentanții numiți de Rețeaua agențiilor UE, la propunerea Comitetului consultativ pentru tehnologia informației și comunicațiilor, informează agențiile și întreprinderile comune ale Uniunii cu privire la deciziile adoptate de IICB. Orice agenție și organ al Uniunii are dreptul să supună atenției reprezentanților și președintelui IICB orice chestiune care, în opinia sa, ar trebui adusă în atenția IICB.

12. IICB poate acționa printr-o procedură scrisă simplificată inițiată de președinte, în temeiul căreia decizia relevantă este considerată aprobată în termenul stabilit de președinte, cu excepția cazului în care un membru formulează obiecții.

13. IICB poate numi un comitet executiv care să îl asiste în activitatea sa și căruia să îi delege o parte din sarcinile și competențele sale. IICB stabilește regulamentul de procedură al comitetului executiv, inclusiv sarcinile și competențele acestuia, precum și mandatul membrilor săi.

Articolul 10
Sarcinile IICB

Când își exercită responsabilitățile, IICB trebuie în special:

(a) să revizuiască eventuale rapoarte solicitate de la CERT-UE cu privire la stadiul punerii în aplicare a prezentului regulament de către instituțiile, organele și agențiile Uniunii;

(b) să aprobe, pe baza unei propuneri din partea șefului CERT-UE, programul anual de lucru al CERT-UE și să monitorizeze implementarea acestuia;

(c) să aprobe, pe baza unei propuneri din partea șefului CERT-UE, catalogul de servicii al CERT-UE;

(d) să aprobe, pe baza unei propuneri din partea șefului CERT-UE, planificarea anuală a veniturilor și cheltuielilor, inclusiv a personalului, pentru activitățile CERT-UE;

(e) să aprobe, pe baza unei propuneri din partea șefului CERT-UE, modalitățile pentru acordurile privind nivelul serviciilor;

(f) să examineze și să aprobe raportul anual întocmit de șeful CERT-UE, referitor la activitățile și gestionarea fondurilor de către CERT-UE;

(g) să aprobe și să monitorizeze indicatorii cheie de performanță pentru CERT-UE, definiți pe baza propunerii șefului CERT-UE;

(h) să aprobe acordurile de cooperare, acordurile privind nivelul serviciilor sau contractele dintre CERT-UE și alte entități în temeiul articolului 17;

(i) să instituie atâtea grupuri consultative tehnice câte sunt necesare pentru a sprijini activitatea IICB, să stabilească mandatul și să desemneze președinții acestor grupuri.

Articolul 11
Respectarea dispozițiilor

IICB monitorizează punerea în aplicare de către instituțiile, organele și agențiile Uniunii a prezentului regulament și a documentelor de orientare, a recomandărilor și a apelurilor la acțiune adoptate. În cazul în care constată că instituțiile, organele sau agențiile Uniunii nu au pus în aplicare în mod eficace prezentul regulament sau documentele de orientare, recomandările și apelurile la acțiune adoptate în temeiul prezentului regulament, IICB poate, fără a aduce atingere procedurilor interne ale instituției, organului sau agenției respective:

(a) să emită un avertisment; dacă este necesar, având în vedere un risc semnificativ de securitate cibernetică, categoria de public căreia i se adresează avertismentul este restricționată în mod corespunzător;

(b) să recomande un serviciu de audit relevant pentru efectuarea unui audit.

Capitolul IV
CERT-UE

Articolul 12
Misiunea și sarcinile CERT-UE

1. Misiunea CERT-UE, a Centrului autonom de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile UE, este de a contribui la securitatea mediului informatic neclasificat al tuturor instituțiilor, organelor și agențiilor Uniunii, oferindu-le consiliere în materie de securitate cibernetică, ajutându-le să prevină, să detecteze, să atenueze și să răspundă la incidente și acționând în calitate de centru de schimb de informații în materie de securitate cibernetică și de coordonare a răspunsului la incidente pentru aceste entități.

2. CERT-UE îndeplinește următoarele sarcini pentru instituțiile, organele și agențiile Uniunii:

   (a) le oferă sprijin pentru punerea în aplicare a prezentului regulament și contribuie la coordonarea punerii în aplicare a prezentului regulament prin intermediul măsurilor enumerate la articolul 13 alineatul (1) sau al rapoartelor ad-hoc solicitate de IICB;

   (b) le oferă sprijin printr-un pachet de servicii de securitate cibernetică descrise în catalogul său de servicii („servicii de referință”);

   (c) menține o rețea de omologi și parteneri pentru a sprijini serviciile, astfel cum se prevede la articolele 16 și 17;

   (d) aduce în atenția IICB orice problemă legată de punerea în aplicare a prezentului regulament și a documentelor de orientare, recomandărilor și apelurilor la acțiune;

   (e) prezintă un raport referitor la amenințările cibernetice cu care se confruntă instituțiile, organele și agențiile Uniunii și contribuie la conștientizarea situației amenințărilor la adresa securității cibernetice în UE.

3. CERT-UE contribuie la activitatea unității cibernetice comune, create în conformitate cu Recomandarea Comisiei din 23 iunie 2021, inclusiv în următoarele domenii:

   (a) pregătirea, coordonarea în materie de incidente, schimbul de informații și răspunsul la situații de criză la nivel tehnic în cazurile legate de instituțiile, organele și agențiile Uniunii;

(b) cooperarea operațională în ceea ce privește rețeaua echipelor de intervenție în caz de incidente de securitate informatică (CSIRT), inclusiv în materie de asistență reciprocă, și comunitatea mai largă a specialiștilor din domeniul securității cibernetice;

(c) informații privind amenințările cibernetice, inclusiv conștientizarea situației;

(d) orice subiect care necesită expertiză tehnică în materie de securitate cibernetică din partea CERT-UE.

4. CERT-UE desfășoară o cooperare structurată cu Agenția Uniunii Europene pentru Securitate Cibernetică în ceea ce privește consolidarea capacităților, cooperarea operațională și analizele strategice pe termen lung ale amenințărilor cibernetice, în temeiul Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului.

5. CERT-UE poate furniza următoarele servicii care nu sunt descrise în catalogul său de servicii („servicii contra cost”):

(a) servicii care sprijină securitatea cibernetică a mediului informatic al instituțiilor, organelor și agențiilor Uniunii, altele decât cele menționate la alineatul (2), în temeiul unor acorduri privind nivelul serviciilor și sub rezerva resurselor disponibile;

(b) servicii care sprijină operațiunile sau proiectele în materie de securitate cibernetică ale instituțiilor, organelor și agențiilor Uniunii, altele decât cele care vizează protejarea mediului lor informatic, în temeiul unor acorduri scrise și cu aprobarea prealabilă a IICB;

(c) servicii care sprijină securitatea mediului informatic al altor organizații decât instituțiile, organele și agențiile Uniunii, care cooperează îndeaproape cu instituțiile, organele și agențiile Uniunii, de exemplu, cărora li s-au atribuit sarcini sau responsabilități în temeiul dreptului Uniunii, în temeiul unor acorduri scrise și cu aprobarea prealabilă a IICB.

6. CERT-UE poate organiza exerciții de securitate cibernetică sau poate recomanda participarea la exercițiile existente, în strânsă cooperare cu Agenția Uniunii Europene pentru Securitate Cibernetică, dacă este cazul, pentru a testa nivelul de securitate cibernetică al instituțiilor, organelor și agențiilor Uniunii.

7. CERT-UE poate oferi instituțiilor, organelor și agențiilor Uniunii asistență referitoare la incidentele din medii informatice clasificate, dacă entitatea în cauză îi solicită acest lucru în mod expres.

Articolul 13

Documente de orientare, recomandări și apeluri la acțiune

1. CERT-UE sprijină punerea în aplicare a prezentului regulament prin adoptarea unor:

(a) apeluri la acțiune care descriu măsurile urgente de securitate pe care instituțiile, organele și agențiile Uniunii sunt invitate să le adopte într-un termen stabilit;

(b) propuneri de documente de orientare, transmise IICB, care se adresează tuturor instituțiilor, organelor și agențiilor Uniunii sau doar unei părți a acestora;

(c) propuneri de recomandări, transmise IICB, care se adresează instituțiilor, organelor și agențiilor individuale ale Uniunii.

2. Documentele de orientare și recomandările pot include:

(a) modalități de sau îmbunătățiri ale gestionării riscurilor de securitate cibernetică și ale nivelului de referință în materie de securitate cibernetică;

(b) modalități de evaluare a nivelului maturității și de elaborare a planurilor de securitate cibernetică; și

(c) după caz, utilizarea tehnologiei și a arhitecturii comune, precum și a celor mai bune practici asociate în scopul realizării interoperabilității și a standardelor comune în sensul articolului 4 punctul 10 din [propunerea de Directivă NIS 2].

3. La propunerea CERT-UE, IICB poate adopta documente de orientare sau recomandări.

4. IICB poate solicita CERT-UE să emită, să retragă sau să modifice o propunere de document de orientare sau de recomandare sau un apel la acțiune.

Articolul 14
Șeful CERT-UE

Șeful CERT-UE prezintă IICB și președintelui IICB rapoarte periodice privind performanța CERT-UE, planificarea financiară, veniturile, execuția bugetară, acordurile privind nivelul serviciilor și acordurile scrise încheiate, cooperarea cu omologii și partenerii și misiunile desfășurate de personal, inclusiv rapoartele menționate la articolul 10 alineatul (1).

Articolul 15
Aspecte financiare și de personal

1. După obținerea unei aprobări unanime din partea IICB, Comisia numește șeful CERT-UE. IICB este consultat în toate etapele procedurii care precede numirea șefului CERT-UE, în special în ceea ce privește elaborarea anunțurilor privind posturile vacante, examinarea dosarelor de candidatură și desemnarea comitetelor de selecție pentru acest post.

2. În ceea ce privește aplicarea procedurilor administrative și financiare, șeful CERT-UE acționează sub autoritatea Comisiei.

3. Sarcinile și activitățile CERT-UE, inclusiv serviciile furnizate de CERT-UE în temeiul articolului 12 alineatele (2), (3), (4) și (6) și al articolului 13 alineatul (1) instituțiilor, organelor și agențiilor Uniunii finanțate în cadrul rubricii „Administrația publică europeană” din cadrul financiar multianual sunt finanțate printr-o linie bugetară separată a bugetului Comisiei. Posturile alocate CERT-UE sunt detaliate într-o notă de subsol la schema de personal a Comisiei.

4. Instituțiile, organele și agențiile Uniunii, altele decât cele menționate la alineatul (3), aduc o contribuție anuală la bugetul CERT-UE pentru a acoperi serviciile furnizate de CERT-UE în temeiul alineatului menționat. Contribuțiile respective se bazează pe orientările oferite de IICB și convenite între fiecare entitate și CERT-UE în cadrul acordurilor privind nivelul serviciilor. Contribuțiile reprezintă un procent echitabil și proporțional din costurile totale ale serviciilor furnizate. Acestea sunt primite în cadrul liniei bugetare separate menționate la alineatul (3) ca venituri alocate, astfel cum se prevede la articolul 21 alineatul (3) litera (c) din Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului[8].

5. Costurile aferente sarcinilor definite la articolul 12 alineatul (5) se recuperează de la instituțiile, organele și agențiile Uniunii beneficiare ale serviciilor furnizate de CERT-UE. Veniturile sunt alocate liniilor bugetare prin care se suportă costurile.

Articolul 16
Cooperarea CERT-UE cu omologii din statele membre

1. CERT-UE cooperează și face schimb de informații cu omologii naționali din statele membre, inclusiv CERT, centrele naționale de securitate cibernetică, CSIRT și punctele unice de contact menționate la articolul 8 din [propunerea de Directivă NIS 2], cu privire la amenințările cibernetice, la vulnerabilități și incidente, la posibilele contramăsuri și la toate aspectele relevante pentru îmbunătățirea protecției mediilor informatice ale instituțiilor, organelor și agențiilor Uniunii, inclusiv prin intermediul rețelei CSIRT menționate la articolul 13 din [propunerea de Directivă NIS 2].

2. CERT-UE poate face schimb de informații referitoare la incidente cu omologii naționali din statele membre pentru a facilita detectarea amenințărilor sau a incidentelor cibernetice similare fără consimțământul entității afectate. CERT-UE poate face schimb de informații referitoare la incidente care dezvăluie identitatea persoanei vizate de incidentul de securitate cibernetică numai cu consimțământul entității afectate.

Articolul 17
Cooperarea CERT-UE cu omologii din statele terțe

1. CERT-UE poate coopera cu omologii din statele terțe, inclusiv cu omologii din cadrul sectorului, cu privire la instrumente și metode, cum ar fi tehnici, tactici, proceduri și bune practici, precum și cu privire la amenințări cibernetice și vulnerabilități. Pentru orice formă de cooperare cu astfel de omologi, inclusiv într-un cadru în care omologii din afara UE cooperează cu omologii naționali din statele membre, CERT-UE solicită aprobarea prealabilă a IICB.

2. CERT-UE poate coopera cu alți parteneri, precum entități comerciale, organizații internaționale, entități naționale din afara Uniunii Europene sau experți individuali,

[8] Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului din 18 iulie 2018 privind normele financiare aplicabile bugetului general al Uniunii, de modificare a Regulamentelor (UE) nr. 1296/2013, (UE) nr. 1301/2013, (UE) nr. 1303/2013, (UE) nr. 1304/2013, (UE) nr. 1309/2013, (UE) nr. 1316/2013, (UE) nr. 223/2014, (UE) nr. 283/2014 și a Deciziei nr. 541/2014/UE și de abrogare a Regulamentului (UE, Euratom) nr. 966/2012 (JO L 193, 30.7.2018, p. 1).

pentru a colecta informații cu privire la amenințările cibernetice generale și specifice, la vulnerabilități și la posibilele contramăsuri. Pentru o cooperare mai extinsă cu astfel de parteneri, CERT-UE solicită aprobarea prealabilă a IICB.

3. Cu acordul entității afectate de un incident, CERT-UE poate să furnizeze informații referitoare la incident partenerilor care pot contribui la analiza acestuia.

Capitolul V
OBLIGAȚII DE COOPERARE ȘI DE RAPORTARE

Articolul 18
Gestionarea informațiilor

1. CERT-UE și instituțiile, organele și agențiile Uniunii respectă obligația de a nu divulga informații care constituie secret profesional, în conformitate cu articolul 339 din Tratatul privind funcționarea Uniunii Europene sau cu cadrele echivalente aplicabile.

2. Dispozițiile Regulamentului (CE) nr. 1049/2001 al Parlamentului European și al Consiliului[9] se aplică în ceea ce privește cererile de acces public la documentele deținute de CERT-UE, inclusiv obligația care decurge din regulamentul menționat de a consulta alte instituții, organe și agenții ale Uniunii ori de câte ori o cerere se referă la documentele lor.

3. Prelucrarea datelor cu caracter personal efectuată în temeiul prezentului regulament face obiectul Regulamentului (UE) 2018/1725 al Parlamentului European și al Consiliului.

4. CERT-UE și instituțiile, organele și agențiile Uniunii gestionează informațiile în conformitate cu normele prevăzute în [propunerea de regulament privind securitatea informațiilor].

5. Orice contact cu CERT-UE inițiat sau solicitat de serviciile naționale de securitate și de informații trebuie comunicat fără întârzieri nejustificate Direcției Securitate a Comisiei și președintelui IICB.

Articolul 19
Obligații privind schimbul de informații

1. Pentru a coordona gestionarea vulnerabilităților și răspunsul la incidente, CERT-UE le poate solicita instituțiilor, organelor și agențiilor Uniunii să îi furnizeze informații din inventarele lor de sisteme informatice care sunt relevante pentru sprijinul CERT-UE. Instituția, organul sau agenția care primește o astfel de solicitare transmite

[9] 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).

informațiile solicitate și orice modificare ulterioară a acestora, fără întârzieri nejustificate.

2. Instituțiile, organele și agențiile Uniunii, la cererea CERT-UE și fără întârzieri nejustificate, îi furnizează informații digitale create prin utilizarea dispozitivelor electronice implicate în incidentele lor respective. CERT-UE poate stabili mai în detaliu tipurile de informații digitale de care are nevoie pentru o cunoaștere detaliată a situației și pentru răspunsul la incidente.

3. CERT-UE poate face schimb de informații referitoare la incidente care dezvăluie identitatea instituției, organului sau agenției Uniunii afectate de incident numai cu consimțământul entității respective. CERT-UE poate face schimb de informații referitoare la incidente care dezvăluie identitatea țintei incidentului de securitate cibernetică numai cu consimțământul entității afectate de incident.

4. Obligațiile privind schimbul de informații nu se aplică în cazul informațiilor UE clasificate (IUEC) și al informațiilor pe care o instituție, un organ sau o agenție a Uniunii le-a primit de la un serviciu de securitate sau de informații al unui stat membru sau de la o agenție de aplicare a legii cu condiția explicită ca acestea să nu fie comunicate CERT-UE.

Articolul 20
Obligații de notificare

1. Toate instituțiile, organele și agențiile Uniunii vor trimite CERT-UE o notificare inițială cu privire la amenințările cibernetice semnificative, vulnerabilitățile semnificative și incidentele semnificative, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la data la care au luat cunoștință de acestea.

   În cazuri justificate corespunzător și în acord cu CERT-UE, instituția, organul sau agenția Uniunii în cauză se poate abate de la termenul prevăzut la paragraful anterior.

2. Instituțiile, organele și agențiile Uniunii transmit apoi către CERT-UE, fără întârzieri nejustificate, detalii tehnice adecvate privind amenințările cibernetice, vulnerabilitățile și incidentele care permit detectarea, răspunsul la incidente sau adoptarea unor măsuri de atenuare. Notificarea include, dacă sunt disponibili:

   (a) indicatorii de compromis relevanți;

   (b) mecanismele de detectare relevante;

   (c) impactul potențial;

   (d) măsurile de atenuare relevante.

3. CERT-UE transmite lunar ENISA un raport de sinteză cu date anonimizate și agregate privind amenințările cibernetice semnificative, vulnerabilitățile semnificative și incidentele semnificative notificate în conformitate cu alineatul (1).

4. IICB poate emite documente de orientare sau recomandări privind modalitățile și conținutul notificării. CERT-UE difuzează detaliile tehnice adecvate pentru a permite

detectarea proactivă, răspunsul la incidente sau adoptarea unor măsuri de atenuare de către instituțiile, organele și agențiile Uniunii.

5. Obligațiile de notificare nu se aplică în cazul informațiilor IUEC și al informațiilor pe care o instituție, un organ sau o agenție a Uniunii le-a primit de la un serviciu de securitate sau de informații al unui stat membru sau de la o autoritate de aplicare a legii cu condiția explicită ca acestea să nu fie comunicate CERT-UE.

Articolul 21

Coordonarea răspunsului la incidente și cooperarea cu privire la incidentele semnificative

1. Acționând în calitate de centru de schimb de informații în materie de securitate cibernetică și de coordonare a răspunsului la incidente, CERT-UE facilitează schimbul de informații cu privire la amenințările cibernetice, vulnerabilități și incidente, între:

   (a) instituțiile, organele și agențiile Uniunii;

   (b) omologii menționați la articolele 16 și 17.

2. CERT-UE facilitează coordonarea între instituțiile, organele și agențiile Uniunii în ceea ce privește răspunsul la incidente, inclusiv prin:

   (a) contribuția la o comunicare externă coerentă;

   (b) asistență reciprocă;

   (c) utilizarea optimă a resurselor operaționale;

   (d) coordonarea cu alte mecanisme de răspuns la situații de criză la nivelul Uniunii.

3. CERT-UE sprijină instituțiile, organele și agențiile Uniunii în ceea ce privește conștientizarea situației amenințărilor cibernetice, a vulnerabilităților și a incidentelor.

4. IICB elaborează orientări privind coordonarea răspunsului la incidente și cooperarea în cazul incidentelor semnificative. În cazul în care se suspectează că un incident este de natură penală, CERT-UE furnizează orientări privind raportarea incidentului către autoritățile de aplicare a legii.

Articolul 22

Atacuri majore

1. CERT-UE coordonează răspunsul instituțiilor, organelor și agențiilor Uniunii la atacuri majore. CERT-UE menține un inventar al expertizei tehnice necesare pentru răspunsul la incidente în cazul unor astfel de atacuri.

2. Instituțiile, organele și agențiile Uniunii contribuie la inventarul expertizei tehnice prin transmiterea unei liste, actualizate anual, de experți disponibili în cadrul

organizațiilor respective, în care sunt detaliate competențele tehnice specifice ale acestora.

3. Cu aprobarea instituțiilor, organelor și agențiilor Uniunii în cauză, CERT-UE poate apela, de asemenea, la experții de pe lista menționată la alineatul (2) pentru a contribui la identificarea răspunsului la un atac major într-un stat membru, în conformitate cu procedurile operaționale ale unității cibernetice comune.

Capitolul VI
DISPOZIȚII FINALE

Articolul 23
Realocare bugetară inițială

Comisia propune realocarea personalului și a resurselor financiare de la instituțiile, organele și agențiile relevante ale Uniunii către bugetul Comisiei. Realocarea produce efecte în același timp cu primul buget adoptat după intrarea în vigoare a prezentului regulament.

Articolul 24
Revizuire

1. IICB, cu sprijinul CERT-UE, raportează periodic Comisiei cu privire la punerea în aplicare a prezentului regulament. IICB poate, de asemenea, să facă recomandări Comisiei pentru a propune modificarea prezentului regulament.

2. Comisia prezintă Parlamentului European și Consiliului un raport privind punerea în aplicare a prezentului regulament în termen de cel mult 48 luni de la data intrării în vigoare a prezentului regulament și, ulterior, o dată la trei ani.

3. Comisia evaluează funcționarea prezentului regulament și prezintă un raport Parlamentului European, Consiliului, Comitetului Economic și Social European și Comitetului Regiunilor nu mai devreme de cinci ani de la data intrării în vigoare.

Articolul 25
Intrarea în vigoare

Prezentul regulament intră în vigoare în a douăzecea 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 Bruxelles,

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Titlul propunerii/inițiativei

1.2. Domeniul (domeniile) de politică vizat(e)

1.3. Obiectul propunerii/inițiativei:

1.4. Obiectiv(e)

1.4.1. Obiectiv(e) general(e)

1.4.2. Obiectiv(e) specific(e)

1.4.3. Rezultatul (rezultatele) și impactul preconizate

1.4.4. Indicatori de performanță

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.

1.5.2. Valoarea adăugată a intervenției Uniunii (aceasta poate rezulta din diferiți factori, de exemplu mai buna coordonare, securitatea juridică, o mai mare eficacitate sau complementaritate). În sensul prezentului punct, „valoarea adăugată a intervenției Uniunii" este valoarea ce rezultă din intervenția Uniunii care depășește valoarea ce ar fi fost obținută dacă ar fi acționat doar statele membre.

1.5.3. Învățăminte desprinse din experiențele anterioare similare

1.5.4. Compatibilitatea cu cadrul financiar multianual și posibilele sinergii cu alte instrumente corespunzătoare

1.5.5. Evaluarea diferitelor opțiuni de finanțare disponibile, inclusiv a posibilităților de realocare a creditelor

1.6. Durata și impactul financiar ale propunerii/inițiativei

1.7. Modul (modurile) de gestiune preconizat(e)

2. MĂSURI DE GESTIUNE

2.1. Dispoziții în materie de monitorizare și de raportare

2.2. Sistemul (sistemele) de gestiune și de control

2.2.1. Justificarea modului (modurilor) de gestiune, a mecanismului (mecanismelor) de punere în aplicare a finanțării, a modalităților de plată și a strategiei de control propuse

2.2.2. Informații privind riscurile identificate și sistemul (sistemele) de control intern instituit(e) pentru atenuarea lor

2.2.3. Estimarea și justificarea raportului cost-eficacitate al controalelor (raportul dintre „costurile controalelor și valoarea fondurilor aferente gestionate”) și evaluarea nivelurilor preconizate ale riscurilor de eroare (la plată și la închidere)

2.3. Măsuri de prevenire a fraudelor și a neregulilor

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

3.1. Rubrica (rubricile) din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate)

3.2. Impactul financiar estimat al propunerii asupra creditelor

3.2.1. Sinteza impactului estimat asupra creditelor operaționale

3.2.2. Realizările preconizate finanțate din credite operaționale

3.2.3. Sinteza impactului estimat asupra creditelor administrative

3.2.4. Compatibilitatea cu cadrul financiar multianual actual

3.2.5. Contribuțiile terților

3.3. Impactul estimat asupra veniturilor

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Titlul propunerii/inițiativei

Propunere de regulament al Parlamentului European și al Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii

1.2. Domeniul (domeniile) de politică vizat(e)

Administrația publică europeană

Propunerea se referă la măsuri care asigură un nivel comun ridicat de securitate cibernetică în instituțiile, organele și agențiile Uniunii

1.3. Obiectul propunerii/inițiativei:

☑o acțiune nouă

☐ o acțiune nouă întreprinsă ca urmare a unui proiect-pilot/a unei acțiuni pregătitoare[10]

☐ prelungirea unei acțiuni existente

☑ o fuziune sau o redirecționare a uneia sau mai multor acțiuni către o altă/o nouă acțiune

1.4. Obiectiv(e)

1.4.1. Obiectiv(e) general(e)

– Instituirea unui cadru pentru asigurarea unui nivel comun ridicat de securitate cibernetică în instituțiile, organele și agențiile Uniunii

– Un nou temei juridic pentru CERT-UE în vederea consolidării mandatului și a finanțării acestuia

1.4.2. Obiectiv(e) specific(e)

(1) Stabilirea de obligații pentru instituțiile, organele și agențiile Uniunii de a institui un cadru intern de gestionare, guvernanță și control al riscurilor de securitate cibernetică

(2) Stabilirea de obligații pentru instituțiile, organele și agențiile Uniunii de a raporta cu privire la cadrul lor intern de gestionare, guvernanță și control al

[10] Astfel cum se menționează la articolul 58 alineatul (2) litera (a) sau (b) din Regulamentul financiar.

riscurilor de securitate cibernetică, precum și cu privire la incidentele de securitate cibernetică

(3) Stabilirea normelor privind organizarea și funcționarea Centrului de securitate cibernetică pentru instituțiile, organele și agențiile Uniunii (CERT-UE) și privind organizarea și funcționarea Consiliului interinstituțional pentru securitate cibernetică (IICB)

(4) Contribuția la unitatea cibernetică comună

1.4.3. Rezultatul (rezultatele) și impactul preconizate

A se preciza efectele pe care propunerea/inițiativa ar trebui să le aibă asupra beneficiarilor vizați/grupurilor vizate.

– Cadre interne de gestionare, guvernanță și control al riscurilor de securitate cibernetică, niveluri de referință în materie de securitate cibernetică, evaluări periodice ale nivelului maturității și planuri de securitate cibernetică ale instituțiilor, organelor și agențiilor Uniunii
– Îmbunătățirea capacității de reziliență în materie de securitate cibernetică și a capacității de răspuns la incidente ale instituțiilor, organelor și agențiilor Uniunii
– Modernizarea CERT-UE
– Contribuția la unitatea cibernetică comună

1.4.4. Indicatori de performanță

A se preciza indicatorii care permit monitorizarea progreselor și a realizărilor obținute.

– Cadre și niveluri de referință instituite, evaluări periodice ale maturității efectuate și planuri de securitate cibernetică elaborate de instituțiile, organele și agențiile Uniunii
– Gestionarea îmbunătățită a incidentelor
– Creșterea gradului de conștientizare a riscurilor de securitate cibernetică la nivelul conducerii superioare a instituțiilor, organelor și agențiilor Uniunii
– Uniformizarea cheltuielilor în materie de securitate TIC ca procent din totalul cheltuielilor TIC
– Autoritate marcantă a IICB și CERT-UE
– Intensificarea schimbului de informații între instituțiile, organele și agențiile Uniunii, precum și cu organismele și părțile interesate relevante din UE
– Intensificarea cooperării în materie de securitate cibernetică cu organismele și părțile interesate relevante din UE, prin intermediul CERT-UE și ENISA

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.

Propunerea are ca obiectiv creșterea nivelului de reziliență cibernetică a instituțiilor, organelor și agențiilor Uniunii, reducerea inconsecvențelor în ceea ce privește reziliența acestor entități și îmbunătățirea nivelului de conștientizare comună a situației și a capacității colective de pregătire și răspuns.

Propunerea este pe deplin consecventă și coerentă cu alte inițiative conexe, în special cu propunerea de directivă privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/1148 [propunerea NIS 2].

Propunerea este o parte esențială a Strategiei UE privind uniunea securității și a Strategiei de securitate cibernetică a UE pentru deceniul digital.

Regulamentul va fi propus de Comisia Europeană în octombrie 2021, adoptarea regulamentului de către Parlamentul European și Consiliu este prevăzută pentru 2022, iar dispozițiile vor fi aplicabile de la data intrării în vigoare a regulamentului. Se preconizează că impactul financiar și în materie de resurse umane prezentat în această fișă financiară legislativă va începe în 2023. O perioadă pregătitoare a început deja în 2021, însă activitățile pregătitoare din 2021 și 2022 nu sunt incluse în impactul financiar al propunerii.

1.5.2. Valoarea adăugată a intervenției Uniunii (aceasta poate rezulta din diferiți factori, de exemplu mai buna coordonare, securitatea juridică, o mai mare eficacitate sau complementaritate). În sensul prezentului punct, „valoarea adăugată a intervenției Uniunii” este valoarea ce rezultă din intervenția Uniunii care depășește valoarea ce ar fi fost obținută dacă ar fi acționat doar statele membre.

Motivele acțiunii la nivel european (ex ante)

În perioada 2019-2021, numărul incidentelor semnificative care au afectat instituțiile, organele și agențiile Uniunii, provocate de actori care generează amenințări persistente avansate a crescut dramatic. În prima jumătate a anului 2021, numărul incidentelor semnificative a fost echivalent cu cel înregistrat pe parcursul întregului an 2020. Acest lucru se reflectă, de asemenea, în numărul de copii conforme (instantanee ale conținutului sistemelor sau dispozitivelor afectate) analizate de CERT-UE în 2020, care s-a triplat în comparație cu 2019, în timp ce numărul incidentelor semnificative a crescut de peste zece ori față de 2018.

Nivelul de maturitate în materie de securitate cibernetică variază substanțial de la o entitate la alta[11]. Prezentul regulament asigură faptul că toate instituțiile, organele și agențiile Uniunii vor pune în aplicare un nivel de referință în materie de securitate cibernetică și vor coopera pentru a asigura funcționarea deschisă și eficientă a administrației Uniunii.

[11] Referință: [Raport special al Curții de Conturi Europene privind securitatea cibernetică în instituțiile, organele și agențiile Uniunii].

Sistemele care trebuie protejate țin de autonomia instituțiilor, organelor și agențiilor Uniunii și sunt operate de acestea; acțiunile propuse nu au putut fi întreprinse de statele membre.

1.5.3. Învățăminte desprinse din experiențele anterioare similare

Directiva NIS a fost primul instrument orizontal al pieței interne care a vizat îmbunătățirea rezilienței rețelelor și a sistemelor din Uniune la riscurile de securitate cibernetică. De când a intrat în vigoare în 2016, directiva a contribuit în mare măsură la creșterea nivelului comun de securitate cibernetică în rândul statelor membre. Propunerea de Directivă NIS2 urmărește să îmbunătățească în continuare aceste măsuri.

Regulamentul urmărește să prevadă măsuri similare pentru instituțiile, organele și agențiile Uniunii.

1.5.4. Compatibilitatea cu cadrul financiar multianual și posibilele sinergii cu alte instrumente corespunzătoare

Propunerea este în concordanță cu cadrul financiar multianual și reprezintă o parte esențială a Strategiei UE privind uniunea securității, precum și a Strategiei de securitate cibernetică a UE pentru deceniul digital.

Propunerea prevede aplicarea de măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele și agențiile Uniunii. Propunerea se aliniază la propunerea de directivă privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/1148 [propunerea NIS 2].

1.5.5. Evaluarea diferitelor opțiuni de finanțare disponibile, inclusiv a posibilităților de realocare a creditelor

Gestionarea sarcinilor de către CERT-UE necesită profiluri specifice și un volum de muncă suplimentar care nu poate fi absorbit fără o creștere a resurselor umane și financiare.

1.6. Durata și impactul financiar ale propunerii/inițiativei

☐ **durată limitată**

– ☐ în vigoare din [ZZ/LL]AAAA până la [ZZ/LL]AAAA

– ☐ impact financiar din AAAA până în AAAA pentru creditele de angajament și din AAAA până în AAAA pentru creditele de plată

☑ **durată nelimitată**

– Impactul financiar ar trebui să înceapă cu primul buget adoptat după intrarea în vigoare a regulamentului. O realocare a resurselor de la instituțiile și principalele organe ale Uniunii către Comisie ar urma să aibă loc în primul an, considerat un an de tranziție; aceasta și alte (re)alocări ale resurselor vor avea loc în cadrul bugetelor anuale. Dacă regulamentul va fi adoptat în 2022, exercițiul financiar 2023 va reprezenta perioada de tranziție, iar în 2024 va începe perioada de funcționare la capacitate maximă.

1.7. Modul (modurile) de gestiune preconizat(e)[12]

☑ **Gestiune directă** asigurată de Comisie și de fiecare instituție, organ și agenție a Uniunii

– ☑ prin intermediul departamentelor 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 agențiile acestora (a se preciza);

– ☐ BEI 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 prezinte garanții financiare adecvate;

[12] Explicații detaliate privind modurile de gestiune, precum și trimiterile la Regulamentul financiar sunt disponibile pe site-ul BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

– ☐ organismelor de drept privat dintr-un stat membru care sunt responsabile cu punerea în aplicare a unui parteneriat public-privat și care prezintă garanții financiare adecvate;

– ☐ persoanelor cărora li se încredințează executarea unor acțiuni specifice în cadrul PESC, în temeiul titlului V din TUE, și care sunt identificate în actul de bază relevant.

– *Dacă se indică mai multe moduri de gestiune, a se furniza detalii suplimentare în secțiunea „Observații”.*

Observații

În ceea ce privește aplicarea procedurilor administrative și financiare, CERT-UE acționează sub autoritatea Comisiei.

Resurse suplimentare care decurg din proiectul de regulament:

Punerea în aplicare a articolelor 12 și 13 din proiectul de regulament presupune extinderea catalogului de servicii cu servicii de referință suplimentare. Pentru funcționarea la capacitate maximă vor fi necesare următoarele resurse suplimentare (până la încheierea CFM, la finalul anului 2027): 21 de ENI și 14,05 milioane EUR.

Resursele suplimentare din buget sunt defalcate în funcție de sarcini după cum urmează:

(a) Pentru îndeplinirea sarcinilor instituțiilor, organelor și agențiilor Uniunii detaliate la articolul 12 alineatul (2) literele (a) - (c) și (e): 13,75 ENI și 11,275 milioane EUR;

(b) Pentru îndeplinirea sarcinilor detaliate la articolul 12 alineatul (3) (contribuția la unitatea cibernetică comună): 2 ENI și 381 000 EUR;

(c) Pentru îndeplinirea sarcinilor detaliate la articolul 12 alineatul (4) (cooperarea structurată cu ENISA): 0,25 ENI și 236 000 EUR;

(d) Pentru îndeplinirea sarcinilor detaliate la articolul 12 alineatul (6) (exerciții de securitate cibernetică): 0,25 ENI și 79 000 EUR;

(e) Pentru îndeplinirea sarcinilor detaliate la articolul 12 alineatul (2) litera (d) și la articolul 13 (analiza și raportarea cu privire la punerea în aplicare a regulamentului, elaborarea de documente de orientare, recomandări și apeluri la acțiune): 3,75 ENI și 2,079 milioane EUR;

(f) Pentru îndeplinirea sarcinilor de sprijinire a secretariatului Consiliului interinstituțional pentru securitate cibernetică (IICB): 1 ENI.

Prezentare generală a resurselor actuale și tranziția către funcționarea la capacitate maximă:

În septembrie 2021, CERT-UE a funcționat cu următoarele resurse:

- posturi permanente și ocupate prin detașare: 14 ENI;

- agenți contractuali finanțați în temeiul acordurilor privind nivelul serviciilor: 24 de ENI;

- în total, 38 de ENI.

În 2020, CERT-UE a avut un buget de: 250 000 EUR din bugetul Comisiei, 3,5 milioane EUR ca venituri alocate în temeiul acordurilor privind nivelul serviciilor. În total: 3,75 milioane EUR. Acesta a constituit întregul buget al CERT-UE, care acoperă formarea, echipamentele hardware, software, misiunile, asistența, agenții contractuali și conferințele.

După intrarea în vigoare a regulamentului, se preconizează că CERT-UE va beneficia de următoarele resurse:

- posturi permanente: 34 de ENI;

- agenți contractuali: 15 ENI;

- în total, 49 de ENI, reprezentând o creștere netă de 11 ENI.

Modificarea raportului dintre posturile permanente și agenții contractuali abordează obstacolul relevant al angajării și păstrării profesioniștilor cu experiență în domeniul securității cibernetice, având în vedere deficitul de astfel de profesioniști pe piața forței de muncă.

În plus, va fi nevoie de 1 agent contractual ENI în cadrul Direcției Generale Informatică a Comisiei pentru a sprijini IICB (Consiliul interinstituțional pentru securitate cibernetică).

Prin urmare, pentru punerea în aplicare a regulamentului sunt necesari 21 de ENI suplimentari (20 de ENI pentru CERT-UE și 1 pentru Direcția Generală Informatică a Comisiei). Acest număr va fi compensat printr-o reducere în paralel a personalului CERT-UE cu 9 agenți contractuali ENI, care au fost finanțați anterior din veniturile alocate în temeiul acordurilor privind nivelul serviciilor.

Bugetul CERT-UE pentru resurse neumane în 2024, după perioada de tranziție, va acoperi sarcinile enumerate mai sus la literele (a)-(e) și se preconizează că va fi finanțat după cum urmează:

- 8,921 milioane EUR pe an de la instituțiile Uniunii finanțate din bugetul Uniunii, rubrica 7;

- 2,459 milioane EUR de la instituțiile, organele și agențiile Uniunii finanțate din bugetul Uniunii, rubricile 1-6;

- 2,670 milioane EUR de la instituțiile, organele și agențiile Uniunii care se autofinanțează.

- Bugetul total al CERT-UE: 14,05 milioane EUR.

Sarcinile enumerate la articolul 12 alineatul (5) nu sunt descrise în catalogul de servicii, acestea fiind servicii contra cost. Acestea sunt servicii auxiliare, reprezintă sume relativ mici, sunt în cea mai mare parte temporare, iar costurile acestor servicii vor fi recuperate de la beneficiarii serviciilor în temeiul unor acorduri privind nivelul serviciilor sau al unor acorduri scrise.

În ceea ce privește contribuțiile la personalul CERT-UE: instituțiile și principalele organe ale Uniunii contribuie în mod echitabil, proporțional cu ponderea respectivă a posturilor AD permanente ale organizației. Ar trebui analizată, de asemenea, posibilitatea ca BCE și BEI să contribuie în mod echitabil prin detașarea de personal permanent.

2. MĂSURI DE GESTIUNE

2.1. Dispoziții în materie de monitorizare și de raportare

A se preciza frecvența și condițiile.

Comisia, cu ajutorul IICB și CERT-UE, va revizui periodic funcționarea regulamentului și va prezenta un raport Parlamentului European și Consiliului, prima dată în termen de cel mult 48 de luni de la intrarea în vigoare a prezentului regulament și, ulterior, o dată la trei ani.

Datele utilizate pentru aceste evaluări vor proveni în principal de la IICB și CERT-UE. În plus, ar putea fi utilizate instrumente specifice de colectare a datelor, dacă este necesar, de exemplu sondaje în rândul instituțiilor, organelor și agențiilor Uniunii, al ENISA sau al rețelei CSIRT.

2.2. Sistemul (sistemele) de gestiune și de control

2.2.1. Justificarea modului (modurilor) de gestiune, a mecanismului (mecanismelor) de punere în aplicare a finanțării, a modalităților de plată și a strategiei de control propuse

Acțiunile întreprinse în temeiul regulamentului vor fi gestionate de fiecare instituție, organ și agenție a Uniunii, în conformitate cu normele și reglementările relevante ale acestora.

Gestiunea administrativă și financiară a activităților CERT-UE este integrată în administrația Comisiei și respectă mecanismele de gestiune și de punere în aplicare, modalitățile de plată și controalele acesteia.

Auditorul intern al Comisiei exercită asupra CERT-UE aceleași prerogative ca și asupra serviciilor Comisiei.

2.2.2. Informații privind riscurile identificate și sistemul (sistemele) de control intern instituit(e) pentru atenuarea lor

Risc foarte scăzut, întrucât CERT-UE este deja subordonat din punct de vedere administrativ, în calitate de grup operativ al Comisiei, directorului general al DG Informatică, iar IICB funcționează după modelul actualului Comitet director al CERT-UE. Prin urmare, ecosistemul de gestiune financiară și control intern există deja.

2.2.3. Estimarea și justificarea raportului cost-eficacitate al controalelor (raportul dintre „costurile controalelor și valoarea fondurilor aferente gestionate”) și evaluarea nivelurilor preconizate ale riscurilor de eroare (la plată și la închidere)

Procedurile de achiziții publice, de gestiune financiară și de control sunt deja instituite și bine testate. Raportul cost-eficacitate al controalelor și nivelurile de risc de eroare corespund celor din fiecare instituție, organ sau agenție a Uniunii, precum și celor ale Comisiei pentru activitățile CERT-UE.

2.3. Măsuri de prevenire a fraudelor și a neregulilor

A se preciza măsurile de prevenire și de protecție existente sau preconizate, de exemplu din strategia antifraudă.

Sistemele de gestiune financiară și de control intern ale Comisiei se aplică activităților CERT-UE.

Pentru a combate fraudele, corupția și alte activități ilegale, dispozițiile Regulamentului (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) se aplică fără restricție.

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. [13]	din partea țărilor AELS[14]	din partea țărilor candidate[15]	din partea țărilor terțe	în sensul articolului 21 alineatul (2) litera (b) din Regulamentul financiar
de la 1 la 6	Linii bugetare care acoperă contribuțiile Uniunii la agențiile și organele descentralizate	Dif.	NU	NU	NU	NU
7	Linii bugetare care acoperă remunerațiile personalului, cheltuielile TI și alte cheltuieli administrative din diferitele secțiuni ale bugetului UE	Nedif.	NU	NU	NU	NU

- Noile linii bugetare solicitate

În ordinea rubricilor din cadrul financiar multianual și a liniilor bugetare.

Rubrica din cadrul financiar multianual	Linia bugetară	Tip de cheltuieli	Contribuție			
	Numărul	Dif./Nedif.	din partea țărilor AELS	din partea țărilor candidate	din partea țărilor terțe	în sensul articolului 21 alineatul (2) litera (b) din Regulamentul financiar
	Niciunul		DA/NU	DA/NU	DA/NU	DA/NU

[13] Dif. = credite diferențiate / Nedif. = credite nediferențiate.
[14] AELS: Asociația Europeană a Liberului Schimb.
[15] Țările candidate și, după caz, candidații potențiali din Balcanii de Vest.

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:

milioane EUR (cu trei zecimale)

Rubrica din cadrul financiar multianual	de la 1 la 6	Rubrici care acoperă contribuțiile la agențiile și organele descentralizate

DG: Mai multe			Anul **2023**	Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**	**TOTAL**
○ Credite operaționale								
Linii bugetare care acoperă contribuțiile Uniunii la agențiile descentralizate (xx 10 xx xx)[16]	Angajamente	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Plăți	(2a)	2,459	2,459	2,459	2,459	2,459	12,293
Credite cu caracter administrativ finanțate din bugetul unor programe specifice[17]								
Linia bugetară		(3)						
TOTAL credite	Angajamente	=1a + 1b + 3	2,459	2,459	2,459	2,459	2,459	12,293

[16] În conformitate cu nomenclatura bugetară oficială.

[17] Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă, cercetare directă.

pentru DG: Mai multe	Plăți	=2a + 2 b +3	2,459	2,459	2,459	2,459	2,459	12,293

○ TOTAL credite operaționale	Angajamente	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Plăți	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ TOTAL credite cu caracter administrativ finanțate din bugetul unor programe specifice		(6)						
TOTAL credite de la RUBRICILE 1 - 6 din cadrul financiar multianual	Angajamente	=4 + 6	2,459	2,459	2,459	2,459	2,459	12,293
	Plăți	=5 + 6	2,459	2,459	2,459	2,459	2,459	12,293

<u>În cazul în care propunerea/inițiativa afectează mai multe rubrici operaționale, a se repeta secțiunea de mai sus:</u>

○ TOTAL credite operaționale (toate rubricile operaționale)	Angajamente	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Plăți	(5)	2,459	2,459	2,459	2,459	2,459	12,293
TOTAL credite cu caracter administrativ finanțate din bugetul unor programe specifice (toate rubricile operaționale)		(6)						
TOTAL credite de la RUBRICILE 1 - 6 din cadrul financiar multianual (Suma de referință)	Angajamente	=4 + 6	2,459	2,459	2,459	2,459	2,459	12,293
	Plăți	=5 + 6	2,459	2,459	2,459	2,459	2,459	12,293

Rubrica din cadrul financiar multianual	**7**	„Cheltuieli administrative”

Această secțiune ar trebui completată utilizând „datele bugetare cu caracter administrativ” care trebuie introduse mai întâi în anexa la fișa financiară legislativă (anexa V la normele interne), încărcată în DECIDE pentru consultarea interservicii.

milioane EUR (cu trei zecimale)

		Anul **2023**	Anul **2024**	Anul **2025**	Anul **2026**	**Anul 2027**	**TOTAL**
DG: DIGIT (CERT-UE)							
○ Resurse umane		1,184	2,126	2,754	3,225	3,225	12,514
○ Alte cheltuieli administrative		7,938	8,921	8,921	8,921	8,921	43,622
TOTAL DG DIGIT (CERT-UE)	Credite	9,122	11,047	11,675	12,146	12,146	56,136

TOTAL credite de la RUBRICA 7 din cadrul financiar multianual	(Total angajamente = Total plăți)	9,122	11,047	11,675	12,146	12,146	**56,136**

milioane EUR (cu trei zecimale)

		Anul 2023	Anul 2024	Anul 2025	Anul 2026	Anul 2027	**TOTAL**
TOTAL credite de la RUBRICILE 1 - 7 din cadrul financiar multianual (*)	Angajamente	11,581	13,506	14,134	14,605	14,605	68,429
	Plăți	11,581	13,506	14,134	14,605	14,605	68,429

(*) Contribuțiile din partea instituțiilor, organelor și agențiilor Uniunii care se autofinanțează sunt estimate la 2,670 milioane EUR pe an (total pentru cei cinci ani: 13,350 milioane EUR). Contribuțiile vor constitui venituri alocate pentru CERT-UE. Tabelele de mai sus includ doar impactul total estimat asupra bugetului Uniunii și nu includ aceste contribuții.

3.2.2. Realizările preconizate finanțate din credite operaționale

Credite de angajament în milioane EUR (cu trei zecimale)

A se indica obiectivele și realizările			Anul **N**		Anul **N+1**		Anul **N+2**		Anul **N+3**		A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)						**TOTAL**	
	REALIZĂRI																	
⇩	Tip[18]	Costuri medii	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Total nr.	Total costuri
OBIECTIVUL SPECIFIC NR. 1[19]…																		
– Realizare																		
– Realizare																		
– Realizare																		
Subtotal pentru obiectivul specific nr. 1																		
OBIECTIVUL SPECIFIC NR. 2…																		
– Realizare																		
Subtotal pentru obiectivul specific nr. 2																		

[18] Realizările se referă la produsele și serviciile care trebuie furnizate (de exemplu: numărul de schimburi de studenți finanțate, numărul de km de drumuri construiți etc.).

[19] Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”

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:

milioane EUR (cu trei zecimale)

	Anul 2023	Anul 2024	Anul 2025	Anul 2026	Anul 2027	**TOTAL**
RUBRICA 7 din cadrul financiar multianual						
Resurse umane						
Personal permanent (grade AD)	1,099	2,041	2,669	3,14	3,14	12,089
Agenți contractuali	0,085	0,085	0,085	0,085	0,085	0,425
Alte cheltuieli administrative	7,938	8,921	8,921	8,921	8,921	43,622
Subtotal de la RUBRICA 7 din cadrul financiar multianual	9,122	11,047	11,675	12,146	12,146	56,136

În afara RUBRICII 7[20] din cadrul financiar multianual						
Resurse umane						
Alte cheltuieli cu caracter administrativ						
Subtotal în afara RUBRICII 7 din cadrul financiar multianual						

TOTAL	9,122	11,047	11,675	12,146	12,146	56,136

Necesarul de credite pentru resursele umane și pentru alte cheltuieli cu caracter administrativ va fi acoperit de creditele direcției generale (DG) respective care sunt deja alocate pentru gestionarea acțiunii și/sau au fost redistribuite intern în DG-ul respectiv, completate, după caz, cu resurse suplimentare care ar putea fi alocate DG-ului care gestionează acțiunea în temeiul procedurii anuale de alocare și ținând seama de constrângerile bugetare.

[20] Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă, cercetare directă.

3.2.3.1. Necesarul de resurse umane estimat

– ☐ Propunerea/inițiativa nu implică utilizarea de resurse umane.

– ☑ Propunerea/inițiativa implică utilizarea de resurse umane, conform explicațiilor de mai jos:

Estimări exprimate în echivalent normă întreagă

		Anul 2023	Anul 2024	Anul 2025	Anul 2026	Anul 2027		
O Posturi din schema de personal (funcționari și agenți temporari)								
20 01 02 01 (la sediu și în reprezentanțele Comisiei)		7	13	17	20	20		
20 01 02 03 (în delegații)								
01 01 01 01 (cercetare indirectă)								
01 01 01 11 (cercetare directă)								
Alte linii bugetare (a se preciza)								
O Personal extern (în echivalent normă întreagă: ENI)[21]								
20 02 01 (AC, END, INT din „pachetul global")		1	1	1	1	1		
20 02 03 (AC, AL, END, INT și JPD în delegații)								
XX 01 xx **yy zz** [22]	- la sediu							
	- în delegații							
01 01 01 02 (AC, END, INT - cercetare indirectă)								
01 01 01 12 (AC, END, INT - cercetare directă)								
Alte linii bugetare (a se preciza)								
TOTAL		**8**	**14**	**18**	**21**	**21**		

XX este domeniul de politică sau titlul din buget în cauză.

Necesarul de resurse umane va fi asigurat din efectivele de personal ale DG-ului în cauză alocate deja pentru gestionarea acțiunii și/sau redistribuite intern în DG, completate, după caz, cu resurse suplimentare ce ar putea fi acordate DG-ului care gestionează acțiunea în temeiul procedurii anuale de alocare și ținând seama de constrângerile bugetare.

Descrierea sarcinilor care trebuie efectuate:

Funcționari și personal temporar	Funcționarii vor implementa sarcinile și activitățile CERT-UE în conformitate cu regulamentul, în special cu capitolele IV și V.
Personal extern	Agentul contractual va sprijini funcțiile de secretariat ale Consiliului interinstituțional pentru securitate cibernetică.

[21] AC = agent contractual; AL = agent local; END = expert național detașat; INT = personal pus la dispoziție de agenți de muncă temporară; JPD = tânăr profesionist în delegații.

[22] Subplafonul pentru personal extern acoperit din creditele operaționale (fostele linii „BA").

3.2.4. Compatibilitatea cu cadrul financiar multianual actual

Propunerea/inițiativa:

– ☑ poate fi finanțată integral prin realocarea creditelor în cadrul rubricii relevante din cadrul financiar multianual (CFM).

A se explica reprogramarea necesară, precizând liniile bugetare în cauză și sumele aferente. Vă rugăm să întocmiți un tabel Excel în cazul unei reprogramări de proporții.

– ☐ necesită utilizarea marjei nealocate din cadrul rubricii corespunzătoare din CFM și/sau utilizarea instrumentelor speciale, astfel cum sunt definite în Regulamentul privind CFM.

A se explica necesitatea efectuării acestei acțiuni, precizând rubricile și liniile bugetare vizate, sumele aferente și instrumentele propuse a fi utilizate.

– ☐ necesită revizuirea CFM.

A se explica necesitatea efectuării acestei acțiuni, precizând rubricile și liniile bugetare vizate, precum și sumele aferente.

3.2.5. Contribuțiile terților

Propunerea/inițiativa:

– ☑ nu prevede cofinanțare din partea terților[23]

– ☐ prevede cofinanțare din partea terților, estimată mai jos:

Credite în milioane EUR (cu trei zecimale)

	Anul **N**[24]	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)			Total
A se preciza organismul care asigură cofinanțarea								
TOTAL credite cofinanțate								

[23] Veniturile alocate provenite din furnizarea sporadică de servicii către organizațiile neconstitutive prevăzute la articolul 12 alineatul (5) litera (c) nu au fost estimate, deoarece ar trebui să fie marginale.

[24] Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei. Vă rugăm să înlocuiți „N” cu primul an estimat de punere în aplicare (de exemplu: 2021). Se procedează la fel pentru anii următori.

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[25]						
		Anul **N**	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)		
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).

[25] 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.