Consiliul
Uniunii Europene

Bruxelles, 24 septembrie 2020
(OR. en)

11051/20

Dosar interinstituțional:
2020/0266 (COD)

EF 228
ECOFIN 846
TELECOM 159
CYBER 168
IA 61
CODEC 871

PROPUNERE

Sursă:	Secretara generală a Comisiei Europene, sub semnătura dlui Jordi AYET PUIGARNAU, Director
Data primirii:	24 septembrie 2020
Destinatar:	Dl Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2020) 595 final
Subiect:	Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014 și (UE) nr. 909/2014

În anexă, se pune la dispoziția delegațiilor documentul COM(2020) 595 final.

Anexă: COM(2020) 595 final

COMISIA
EUROPEANĂ

Bruxelles, 24.9.2020
COM(2020) 595 final

2020/0266 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014 și (UE) nr. 909/2014

(Text cu relevanță pentru SEE)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

- Motivele și obiectivele propunerii

Prezenta propunere face parte din pachetul privind finanțele digitale, un pachet de măsuri menit să faciliteze și să sprijine în continuare potențialul finanțelor digitale în ceea ce privește inovarea și concurența, reducând, în același timp, riscurile care decurg din acestea. Propunerea este în concordanță cu prioritățile Comisiei de a adapta Europa la era digitală și de a construi o economie pregătită pentru viitor, care să funcționeze pentru cetățeni. Pachetul privind finanțele digitale include o nouă strategie privind finanțele digitale pentru sectorul financiar al UE[1], vizând a asigura că UE adoptă revoluția digitală și o propulsează cu firme europene inovatoare în prim-plan, beneficiile finanțelor digitale fiind astfel puse la dispoziția consumatorilor și a întreprinderilor. Pe lângă prezenta propunere, pachetul include, de asemenea, o propunere de regulament privind piețele de criptoactive[2], o propunere de regulament privind un regim-pilot pentru infrastructurile pieței bazate pe tehnologia registrelor distribuite[3] (*distributed ledger technology* – DLT) și o propunere de directivă pentru a clarifica sau a modifica anumite norme conexe privind serviciile financiare din UE[4]. Digitalizarea și reziliența operațională în sectorul financiar sunt două fețe ale aceleiași monede. Tehnologiile digitale sau tehnologiile informației și comunicațiilor (TIC) generează oportunități, dar și riscuri. Acestea trebuie să fie bine înțelese și gestionate, în special în perioade de criză.

Prin urmare, responsabilii de elaborarea politicilor și autoritățile de supraveghere s-au axat tot mai mult pe riscurile care decurg din dependența de TIC. Aceștia au încercat în special să îmbunătățească reziliența întreprinderilor prin stabilirea de standarde și prin coordonarea activității de reglementare sau de supraveghere. Această activitate s-a desfășurat atât la nivel internațional, cât și la nivel european și atât la nivelul industriilor, cât și al anumitor sectoare, inclusiv al serviciilor financiare.

Cu toate acestea, riscurile TIC continuă să reprezinte o provocare pentru reziliența operațională, performanța și stabilitatea sistemului financiar al UE. Reforma care a urmat crizei financiare din 2008 a consolidat în primul rând reziliența financiară[5] a sectorului financiar al UE, abordând riscurile TIC doar indirect în anumite domenii, ca parte a măsurilor de abordare a riscurilor operaționale în sens mai larg.

Deși modificările de după criză aduse legislației UE în domeniul serviciilor financiare au instituit un cadru unic de reglementare care reglementează o mare parte a riscurilor financiare asociate serviciilor financiare, acestea nu au abordat integral reziliența operațională digitală.

---

1 Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor referitoare la Strategia UE privind finanțele digitale, 24 septembrie 2020, COM(2020)591.

2 Propunere de Regulament al Parlamentului European și al Consiliului privind piețele criptoactivelor și de modificare a Directivei (UE) 2019/1937, COM(2020) 593.

3 Propunere de Regulament al Parlamentului European și al Consiliului privind un regim-pilot pentru infrastructurile pieței bazate pe tehnologia registrelor distribuite, COM(2020) 594.

4 Propunere de Directivă a Parlamentului European și al Consiliului de modificare a Directivelor 2006/43/CE, 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 și (UE) 2016/2341, COM(2020) 596.

5 Diferitele măsuri adoptate au vizat în mod fundamental creșterea resurselor de capital și a lichidității entităților financiare, precum și reducerea riscurilor de piață și a riscurilor de credit.

Măsurile luate în legătură cu aceasta din urmă au fost caracterizate de o serie de elemente care au limitat eficacitatea lor. De exemplu, măsurile au fost adesea concepute sub forma unor directive de armonizare minimă sau a unor reglementări bazate pe principii, lăsând loc substanțial pentru abordări divergente în cadrul pieței unice. În plus, riscurile TIC au fost vizate numai într-o măsură limitată sau incompletă, în contextul acoperirii riscului operațional. În cele din urmă, aceste măsuri variază în cadrul legislației sectoriale privind serviciile financiare. Prin urmare, intervenția la nivelul Uniunii nu a corespuns pe deplin cu nevoile entităților financiare europene în ceea ce privește gestionarea riscurilor operaționale într-un mod care să asigure rezistența și răspunsul la impactul incidentelor TIC, precum și redresarea în urma acestora. De asemenea, aceasta nu a furnizat autorităților de supraveghere financiară instrumentele cele mai adecvate pentru a-și îndeplini mandatele de prevenire a instabilității financiare generate de materializarea riscurilor TIC respective.

Absența unor norme detaliate și cuprinzătoare privind reziliența operațională digitală la nivelul UE a condus la proliferarea inițiativelor naționale de reglementare (de exemplu, cu privire la testarea rezilienței operaționale digitale) și la abordări în materie de supraveghere (de exemplu, abordarea dependențelor de furnizori terți de servicii TIC). Totuși, acțiunea la nivelul statelor membre are doar un efect limitat, având în vedere caracterul transfrontalier al riscurilor TIC. În plus, inițiativele naționale necoordonate s-au soldat cu suprapuneri, inconsecvențe, cerințe repetitive, costuri administrative și de conformare ridicate – în special pentru entitățile financiare transfrontaliere – sau cu riscuri TIC rămase nedetectate și, prin urmare, neabordate. Această situație fragmentează piața unică, subminează stabilitatea și integritatea sectorului financiar al UE și periclitează protecția consumatorilor și a investitorilor.

Prin urmare, este necesar să se instituie un cadru detaliat și cuprinzător privind reziliența operațională digitală pentru entitățile financiare din UE. Acest cadru va aprofunda dimensiunea digitală a gestionării riscurilor în cadrul unic de reglementare. În special, acesta va consolida și va raționaliza modul în care entitățile financiare gestionează riscurile TIC, va stabili o testare amănunțită a sistemelor TIC, va spori gradul de conștientizare a autorităților de supraveghere cu privire la riscurile cibernetice și incidentele legate de TIC cu care se confruntă entitățile financiare și va introduce competențe pentru autoritățile de supraveghere financiară în scopul monitorizării riscurilor care decurg din dependența entităților financiare de furnizorii terți de servicii TIC. Propunerea va crea un mecanism coerent de raportare a incidentelor, care va contribui la reducerea sarcinilor administrative pentru entitățile financiare și va consolida eficacitatea supravegherii.

- Coerența cu dispozițiile deja existente în domeniul de politică vizat

Prezenta propunere face parte dintr-o activitate mai amplă desfășurată în prezent la nivel european și internațional în vederea consolidării securității cibernetice în domeniul serviciilor financiare și a abordării riscurilor operaționale mai ample[6].

Aceasta constituie, de asemenea, un răspuns la avizul tehnic comun din 2019[7] al autorităților europene de supraveghere (AES), care au solicitat o abordare mai coerentă în soluționarea riscurilor TIC în domeniul financiar și au recomandat Comisiei să consolideze, în mod proporțional, reziliența operațională digitală a industriei serviciilor financiare prin intermediul

[6] Comitetul de la Basel pentru supraveghere bancară, *Cyber-resilience: Range of practices*, decembrie 2018 și *Principles for sound management of operational risk (PSMOR)*, octombrie 2014.

[7] Avizul comun al autorităților europene de supraveghere adresat Comisiei Europene cu privire la necesitatea unor îmbunătățiri legislative legate de cerințele privind gestionarea riscurilor TIC în sectorul financiar al UE, JC 2019 26 (2019).

unei inițiative sectoriale a UE. Avizul AES a fost un răspuns la Planul de acțiune al Comisiei din 2018 privind FinTech[8].

- Coerența cu alte domenii de politică ale Uniunii

După cum a afirmat președinta von der Leyen în orientările sale politice[9] și după cum s-a stabilit în comunicarea „Conturarea viitorului digital al Europei”[10], este esențial ca Europa să beneficieze de toate avantajele erei digitale și să își consolideze capacitatea industrială și de inovare, fără a transgresa însă limitele siguranței și ale eticii. Strategia europeană privind datele[11] stabilește patru piloni – protecția datelor, drepturile fundamentale, siguranța și securitatea cibernetică – drept condiții prealabile esențiale pentru o societate autonomizată prin utilizarea datelor. În ultima perioadă, Parlamentul European lucrează la un raport privind finanțele digitale, care, printre altele, solicită o abordare comună privind reziliența cibernetică a sectorului financiar[12]. Un cadru legislativ care să consolideze reziliența operațională digitală a entităților financiare din UE este în concordanță cu aceste obiective de politică. Propunerea ar sprijini, de asemenea, politicile care vizează redresarea în urma pandemiei de COVID-19, deoarece ar asigura faptul că dependența sporită de finanțe digitale merge mână în mână cu reziliența operațională.

Inițiativa ar menține beneficiile asociate cadrului orizontal privind securitatea cibernetică (de exemplu, Directiva privind securitatea rețelelor și a sistemelor informatice, Directiva NIS) prin păstrarea sectorului financiar în domeniul său de aplicare. Sectorul financiar ar rămâne strâns asociat cu organismul de cooperare în domeniul NIS, iar autoritățile de supraveghere financiară ar fi în măsură să facă schimb de informații relevante în cadrul ecosistemului NIS existent. Inițiativa ar fi în concordanță cu Directiva privind infrastructura critică europeană (ICE), care este în prezent în curs de revizuire pentru a spori protecția și reziliența infrastructurilor critice împotriva amenințărilor care nu sunt legate de domeniul cibernetic. În cele din urmă, prezenta propunere este pe deplin în concordanță cu Strategia privind o uniune a securității[13] care a solicitat o inițiativă privind reziliența operațională digitală a sectorului financiar, dat fiind gradul său ridicat de dependență de serviciile TIC și vulnerabilitatea sa la atacurile cibernetice.

2. TEMEIUL JURIDIC, SUBSIDIARITATEA ȘI PROPORȚIONALITATEA

- Temeiul juridic

Propunerea de regulament se bazează pe articolul 114 din TFUE.

---

8 Comisia Europeană, *Planul de acțiune privind FinTech*, COM/2018/0109 final.

9 Președinta Ursula Von Der Leyen, Orientări politice pentru următoarea Comisie, 2019-2024, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_ro.pdf.

10 „Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor, *Conturarea viitorului digital al Europei*, COM(2020) 67 final.

11 Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor, *O strategie europeană privind datele*, COM(2020) 66 final.

12 „Raport conținând recomandări adresate Comisiei privind sectorul finanțelor digitale: riscuri emergente în ceea ce privește criptoactivele – provocări în materie de reglementare și de supraveghere în domeniul serviciilor, instituțiilor și piețelor financiare (2020/2034(INL)), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en.

13 Comunicarea Comisiei către Parlamentul European, Consiliul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor referitoare la Strategia UE privind uniunea securității, COM(2020) 605 final.

Aceasta elimină obstacolele din calea instituirii și funcționării pieței interne de servicii financiare și îmbunătățește instituirea și funcționarea acesteia prin armonizarea normelor aplicabile în domeniul gestionării riscurilor TIC, al raportării și testării cu privire la acestea și al riscurilor generate de furnizori terți de servicii TIC. Disparitățile actuale în acest domeniu, atât la nivel legislativ, cât și la nivelul supravegherii, precum și la nivel național și european, acționează ca obstacole în calea pieței unice a serviciilor financiare, deoarece entitățile financiare care desfășoară activități transfrontaliere se confruntă cu cerințe de reglementare diferite, atunci când nu se suprapun, sau cu așteptări în materie de supraveghere care pot împiedica exercitarea libertăților de stabilire și de a presta servicii. Normele diferite denaturează, de asemenea, concurența dintre același tip de entități financiare din diferite state membre. În plus, în domeniile în care armonizarea este absentă, parțială sau limitată, dezvoltarea unor norme sau abordări naționale divergente, aflate fie deja în vigoare, fie în proces de adoptare și de punere în aplicare la nivel național, poate acționa ca factor de descurajare în ceea ce privește libertățile aplicabile pe piața unică pentru serviciile financiare. Acest lucru este valabil în special în ceea ce privește cadrele de testare operațională digitală și supravegherea furnizorilor terți esențiali de servicii TIC.

Întrucât propunerea are impact asupra mai multor directive ale Parlamentului European și ale Consiliului, adoptate în temeiul articolului 53 alineatul (1) din TFUE, se adoptă în același timp o propunere de directivă pentru a reflecta modificările care trebuie aduse directivelor respective.

- Subsidiaritatea

Un nivel ridicat de interconectare între serviciile financiare, o activitate transfrontalieră semnificativă a entităților financiare și o dependență extinsă a sectorului financiar în ansamblu de furnizorii terți de servicii TIC necesită o reziliență operațională digitală puternică, ca o chestiune de interes comun, pentru a susține soliditatea piețelor financiare ale UE. Disparitățile care rezultă din regimuri inegale sau parțiale, suprapuneri sau cerințe multiple care se aplică acelorași entități financiare care desfășoară activități transfrontaliere sau care dețin mai multe autorizații[14] în cadrul pieței unice pot fi abordate în mod eficient numai la nivelul Uniunii.

Prezenta propunere armonizează componenta operațională digitală a unui sector profund integrat și interconectat, care beneficiază deja de un set unic de norme și de supraveghere în majoritatea celorlalte domenii-cheie. În chestiuni precum raportarea incidentelor legate de TIC, numai normele armonizate ale Uniunii ar putea reduce nivelul sarcinilor administrative și al costurilor financiare asociate raportării aceluiași incident legat de TIC către diferite autorități naționale și ale Uniunii. Este necesar să se ia măsuri la nivelul UE pentru a facilita, de asemenea, recunoașterea reciprocă a rezultatelor testelor avansate privind reziliența operațională digitală pentru entitățile care desfășoară activități transfrontaliere, care, în absența unor norme ale Uniunii, intră sau pot intra sub incidența unor cadre diferite din state membre diferite. Numai acțiunea la nivelul Uniunii poate soluționa diferențele dintre abordările de testare introduse de statele membre. Acțiunea la nivelul UE este, de asemenea, necesară pentru a aborda lipsa unor competențe de supraveghere adecvate pentru monitorizarea riscurilor generate de furnizorii terți de servicii TIC, inclusiv a riscurilor de concentrare și de contagiune pentru sectorul financiar al UE.

[14] Aceeași entitate financiară poate avea o autorizație bancară, de firmă de investiții și de instituție de plată, fiecare emisă de o autoritate de supraveghere diferită în unul sau mai multe state membre.

- Proporționalitatea

Normele propuse nu depășesc ceea ce este necesar pentru a atinge obiectivele propunerii. Acestea acoperă numai aspectele pe care statele membre nu le pot realiza pe cont propriu și situațiile în care sarcina administrativă și costurile sunt proporționale cu obiectivele specifice și generale care trebuie atinse.

Proporționalitatea este concepută ținând seama de domeniul de aplicare și de intensitate, prin utilizarea unor criterii de evaluare calitative și cantitative. Acestea vizează să asigure că, deși noile norme acoperă toate entitățile financiare, acestea sunt în același timp adaptate la riscurile și nevoile caracteristicilor lor specifice din punctul de vedere al dimensiunii și al profilurilor de afaceri. Proporționalitatea este, de asemenea, integrată în normele privind gestionarea riscurilor TIC, testarea rezilienței digitale, raportarea incidentelor majore legate de TIC și supravegherea furnizorilor terți esențiali de servicii TIC.

- Alegerea instrumentului

Măsurile necesare pentru reglementarea gestionării riscurilor TIC, a raportării incidentelor legate de TIC, a testării și a supravegherii furnizorilor terți esențiali de servicii TIC trebuie să fie cuprinse într-un regulament, pentru a se asigura că cerințele detaliate sunt aplicabile în mod efectiv, direct și uniform, fără a aduce atingere proporționalității și normelor specifice prevăzute de prezentul regulament. Consecvența în abordarea riscurilor operaționale digitale contribuie la consolidarea încrederii în sistemul financiar și menține stabilitatea acestuia. Întrucât utilizarea unui regulament ajută la reducerea complexității normative, favorizează convergența în materie de supraveghere și sporește securitatea juridică, prezentul regulament contribuie, de asemenea, la limitarea costurilor de conformitate ale entităților financiare, în special pentru cele care funcționează la nivel transfrontalier, ceea ce, la rândul său, ar contribui la eliminarea denaturărilor concurenței.

Prezentul regulament îndepărtează, de asemenea, disparitățile legislative și abordările naționale neuniforme în materie de reglementare sau de supraveghere în ceea ce privește riscurile TIC și elimină astfel obstacolele din calea pieței unice a serviciilor financiare, în special a exercitării fără sincope a libertății de stabilire și de prestare de servicii pentru entitățile financiare cu o prezență transfrontalieră.

În cele din urmă, cadrul unic de reglementare a fost dezvoltat în cea mai mare parte prin regulamente, iar actualizarea sa cu componenta privind reziliența operațională digitală ar trebui să urmeze aceeași alegere privind instrumentul juridic.

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

- Evaluările ex post/verificarea adecvării legislației existente

Până în prezent, legislația Uniunii privind serviciile financiare nu s-a concentrat pe reziliența operațională și niciun act legislativ nu a abordat în mod cuprinzător riscurile care decurg din digitalizare, nici chiar cele ale căror norme abordează mai general dimensiunea riscului operațional în cadrul căruia riscurile TIC constituie o subcomponentă. Până în prezent, intervenția Uniunii a contribuit la abordarea nevoilor și a problemelor existente în urma crizei financiare din 2008: instituțiile de credit nu au fost capitalizate suficient, piețele financiare nu au fost integrate suficient și armonizarea până la momentul respectiv a fost menținută la un nivel minim. Riscurile TIC nu erau considerate atunci o prioritate și, prin urmare, cadrele juridice pentru diferitele subsectoare financiare au evoluat în mod necoordonat. Totuși,

acțiunea Uniunii și-a atins obiectivele privind asigurarea stabilității financiare și instituirea unui set unic de norme armonizate în materie prudențială și de conduită pe piață, aplicabile entităților financiare din întreaga UE. Întrucât factorii care au determinat în trecut intervenția legislativă a Uniunii nu au permis ca norme specifice sau cuprinzătoare să abordeze utilizarea răspândită a tehnologiilor digitale și riscurile aferente în domeniul finanțelor, efectuarea unei evaluări explicite pare dificilă. Un exercițiu implicit de evaluare și modificările legislative care decurg din acesta sunt reflectate în fiecare pilon al prezentului regulament.

- Consultările cu părțile interesate

Comisia a consultat părțile interesate pe tot parcursul procesului de elaborare a prezentei propuneri, în special:

(i) Comisia a organizat o consultare publică deschisă în acest scop (19 decembrie 2019-19 martie 2020)[15];

(ii) Comisia a consultat opinia publică prin intermediul unei evaluări inițiale a impactului (19 decembrie 2019-16 ianuarie 2020)[16];

(iii) Serviciile Comisiei au consultat în două rânduri (18 mai 2020 și 16 iulie 2020) experții statelor membre în cadrul Grupului de experți în materie de servicii bancare, asigurări și plăți (*Expert Group on Banking, Payments and Insurance* – EGBPI)[17];

(iv) Serviciile Comisiei au organizat un webinar dedicat rezilienței operaționale digitale, în cadrul seriei din 2020 de evenimente de informare cu privire la finanțele digitale (19 mai 2020).

Scopul consultării publice a fost acela de a informa Comisia cu privire la dezvoltarea unui potențial cadru intersectorial al UE privind reziliența operațională digitală în domeniul serviciilor financiare. Răspunsurile au arătat un sprijin larg pentru introducerea unui cadru specific cu măsuri axate pe cele patru domenii care fac obiectul consultării, subliniind, în același timp, nevoia de a asigura proporționalitatea și de a aborda și a explica cu atenție interacțiunea cu normele orizontale ale Directivei NIS. Comisia a primit două răspunsuri privind evaluarea inițială a impactului, în cadrul cărora respondenții au abordat aspecte specifice legate de domeniul lor de activitate.

Statele membre au exprimat, în cadrul reuniunii EGBPI, organizate la 18 mai 2020, un sprijin puternic pentru consolidarea rezilienței operaționale digitale a sectorului financiar prin măsurile prevăzute în cele patru elemente prezentate de Comisie. Statele membre au subliniat, de asemenea, necesitatea unei articulări clare a noilor norme cu cele referitoare la riscul operațional (în cadrul legislației UE privind serviciile financiare) și cu normele orizontale privind securitatea cibernetică (Directiva NIS). În cadrul celei de a doua reuniuni, unele state membre au subliniat nevoia de a asigura proporționalitatea și de a analiza situația specifică a întreprinderilor mici sau a filialelor grupurilor mai mari, precum și necesitatea de a avea un mandat puternic pentru autoritățile naționale competente implicate în supraveghere.

---

15 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation.

16 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-.

17 https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en.

Propunerea se bazează, de asemenea, pe observațiile formulate în cadrul reuniunilor cu părțile interesate și cu autoritățile și instituțiile UE și integrează aceste observații. Părțile interesate, inclusiv furnizorii terți de servicii TIC, s-au exprimat, în general, în favoarea propunerii. O analiză a feedbackului primit arată că accentul este pus pe menținerea proporționalității și pe respectarea unei abordări bazate pe principii și pe riscuri în elaborarea normelor. Din punct de vedere instituțional, principalele contribuții au venit din partea Comitetului european pentru risc sistemic (CERS), a AES, a Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) și a Băncii Centrale Europene (BCE), precum și din partea autorităților competente ale statelor membre.

- Obținerea și utilizarea cunoștințelor de specialitate

În pregătirea prezentei propuneri, Comisia s-a bazat pe dovezi calitative și cantitative colectate din surse recunoscute, inclusiv cele două avize tehnice comune ale AES. Acestea au fost completate cu informații confidențiale și cu rapoarte puse la dispoziția publicului de către autoritățile de supraveghere, organismele internaționale de standardizare și institute de cercetare de vârf, precum și cu o contribuție cantitativă și calitativă din partea părților interesate identificate la nivelul sectorului financiar mondial.

- Evaluarea impactului

Prezenta propunere este însoțită de o evaluare a impactului[18], care a fost prezentată Comitetului de control normativ (CCN) la 29 aprilie 2020 și aprobată la 29 mai 2020. CCN a recomandat îmbunătățiri în anumite domenii cu scopul de: (i) a furniza mai multe informații cu privire la modul în care ar fi asigurată proporționalitatea; (ii) a evidenția mai bine măsura în care opțiunea preferată diferă de avizul tehnic comun al AES și motivul pentru care opțiunea respectivă este cea optimă; și (iii) a evidenția în detaliu modul în care propunerea interacționează cu legislația existentă a UE, inclusiv cu normele care sunt în prezent în curs de revizuire. Evaluarea impactului a fost ajustată pentru a aborda aceste aspecte, vizând, de asemenea, observațiile mai detaliate ale CCN.

Comisia a luat în considerare o serie de opțiuni de politică pentru elaborarea unui cadru privind reziliența operațională digitală:

- „Nicio măsură”: normele privind reziliența operațională ar fi stabilite în continuare de setul actual, divergent, de dispoziții ale UE privind serviciile financiare, parțial de Directiva NIS, precum și de regimurile naționale existente sau viitoare;
- Opțiunea 1: consolidarea amortizoarelor de capital: ar fi introduse amortizoare suplimentare de capital pentru a spori capacitatea entităților financiare de a absorbi pierderile care ar putea apărea din cauza lipsei rezilienței operaționale digitale;
- Opțiunea 2: introducerea unui act privind reziliența operațională digitală a serviciilor financiare: punerea în aplicare a unui cadru cuprinzător la nivelul UE, cu norme coerente care să abordeze nevoile de reziliență operațională digitală ale tuturor entităților financiare reglementate și instituirea unui cadru de supraveghere pentru furnizorii terți esențiali de servicii TIC;

[18] Document de lucru al serviciilor Comisiei – Raport de evaluare a impactului care însoțește documentul intitulat „Propunere de regulament al Parlamentului European și al Consiliului privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014 și (UE) nr. 909/2014”, SWD(2020)198, 24.9.2020.

- Opțiunea 3: un act privind reziliența operațională digitală a serviciilor financiare, combinat cu supravegherea centralizată a furnizorilor terți esențiali de servicii TIC: pe lângă actul privind reziliența operațională digitală (opțiunea 2), ar fi instituită o nouă autoritate care să supravegheze furnizarea de servicii de către furnizorii terți de servicii TIC.

A doua opțiune a fost reținută deoarece atinge majoritatea obiectivelor avute în vedere într-un mod eficace, eficient și coerent cu alte politici ale Uniunii. Majoritatea părților interesate preferă, de asemenea, această opțiune.

Opțiunea reținută ar genera costuri atât punctuale, cât și recurente[19]. Costurile punctuale se datorează, în principal, investițiilor în sisteme informatice și, ca atare, sunt dificil de cuantificat având în vedere diversitatea peisajelor informatice complexe ale întreprinderilor și, în special, sistemele lor informatice existente. Chiar și în aceste condiții, este probabil ca aceste costuri să fie limitate pentru întreprinderile mari, având în vedere investițiile semnificative deja realizate în domeniul TIC. De asemenea, se preconizează că, pentru întreprinderile mai mici, costurile vor fi limitate, deoarece s-ar aplica măsuri proporționale, având în vedere gradul lor de risc mai scăzut.

Opțiunea reținută ar avea efecte pozitive asupra IMM-urilor care își desfășoară activitatea în sectorul serviciilor financiare, în ceea ce privește impactul economic, social și de mediu. Propunerea va aduce clarificări IMM-urilor cu privire la normele aplicabile, ceea ce va reduce costurile de conformitate.

Principalul impact social al opțiunii de politică reținute s-ar resimți la nivelul consumatorilor și investitorilor. Nivelurile mai ridicate de reziliență operațională digitală a sistemului financiar al UE ar reduce numărul și costurile medii ale incidentelor. Societatea în ansamblu ar beneficia de creșterea încrederii în sectorul serviciilor financiare.

În cele din urmă, în ceea ce privește impactul asupra mediului, opțiunea de politică aleasă ar încuraja o utilizare sporită a celei mai recente generații de infrastructuri și servicii TIC, care ar trebui să devină mai durabile din punctul de vedere al mediului.

- Adecvarea și simplificarea reglementărilor

Eliminarea cerințelor care se suprapun referitoare la raportarea incidentelor legate de TIC ar reduce sarcinile administrative și costurile asociate. În plus, testarea armonizată a rezilienței operaționale digitale cu o recunoaștere reciprocă în cadrul pieței unice va reduce costurile, în special pentru întreprinderile transfrontaliere care, în caz contrar, s-ar putea confrunta cu obligația efectuării de teste în multe state membre[20].

- Drepturile fundamentale

UE se angajează să respecte standarde ridicate de protecție a drepturilor fundamentale. Toate acordurile voluntare de schimb de informații dintre entitățile financiare pe care prezentul regulament le promovează ar fi realizate în medii de încredere, cu respectarea deplină a normelor Uniunii privind protecția datelor, îndeosebi a Regulamentului (UE) 2016/679 al

[19] *Ibidem, p. 89-94*.
[20] *Ibidem*.

Parlamentului European și al Consiliului[21], în special atunci când prelucrarea datelor cu caracter personal este necesară în scopuri de interes legitim urmărite de operator.

4. IMPLICAȚIILE BUGETARE

În ceea ce privește implicațiile bugetare, întrucât regulamentul actual prevede un rol consolidat al AES prin competențele care le sunt conferite în vederea supravegherii în mod adecvat a furnizorilor terți esențiali de servicii TIC, propunerea ar implica mobilizarea unor resurse sporite, în special pentru a îndeplini misiunile de supraveghere (cum ar fi inspecțiile la fața locului și online și exercițiile de audit), și utilizarea personalului care deține expertiză specifică în domeniul securității TIC.

Volumul și repartizarea acestor costuri vor depinde de amploarea noilor competențe de supraveghere și de sarcinile (precise) care urmează să fie îndeplinite de AES. În ceea ce privește furnizarea de noi resurse de personal, ABE, ESMA și EIOPA vor necesita, în total, 18 angajați cu normă întreagă (ENI) – 6 ENI pentru fiecare autoritate – atunci când vor intra în vigoare diferitele dispoziții ale propunerii (costul fiind estimat la 15,71 milioane EUR pentru perioada 2022-2027). AES vor suporta, de asemenea, costuri IT suplimentare, cheltuieli de misiune pentru inspecțiile la fața locului și costuri de traducere (estimate la 12 milioane EUR pentru perioada 2022-2027), precum și alte cheltuieli administrative (estimate la 2,48 milioane EUR pentru perioada 2022-2027). Prin urmare, impactul total estimat al costurilor este de aproximativ 30,19 milioane EUR pentru perioada 2022-2027.

De asemenea, ar trebui remarcat faptul că, deși numărul de angajați (de exemplu, noi membri ai personalului și alte cheltuieli legate de noile sarcini) necesari pentru supravegherea directă va depinde în timp de evoluția numărului și a dimensiunii furnizorilor terți esențiali de servicii TIC care trebuie supravegheați, cheltuielile respective vor fi finanțate integral din taxele percepute de la respectivii participanți pe piață. Prin urmare, nu este prevăzut un impact asupra creditelor bugetare ale UE (mai puțin în cazul personalului suplimentar), deoarece aceste costuri vor fi finanțate integral din taxe.

Impactul financiar și cel bugetar ale prezentei propuneri sunt explicate în detaliu în fișa financiară legislativă anexată la prezenta propunere.

5. ALTE ELEMENTE

- Planuri de punere în aplicare și modalități de monitorizare, evaluare și raportare

Propunerea include un plan general de monitorizare și evaluare a impactului asupra obiectivelor specifice, solicitând Comisiei să efectueze o revizuire după cel puțin trei ani de la intrarea în vigoare și să raporteze Parlamentului European și Consiliului cu privire la principalele sale constatări.

Evaluarea trebuie efectuată în conformitate cu orientările Comisiei privind o mai bună legiferare.

- Explicații detaliate cu privire la dispozițiile specifice ale propunerii

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

Propunerea este structurată în jurul mai multor domenii de politică principale care sunt piloni interconectați esențiali, incluși în mod consensual în orientările și cele mai bune practici europene și internaționale menite să sporească reziliența cibernetică și operațională a sectorului financiar.

Domeniul de aplicare al regulamentului și aplicarea măsurilor necesare ținând seama de principiul proporționalității (articolul 2)

Pentru a asigura coerența în legătură cu cerințele privind gestionarea riscurilor TIC aplicabile sectorului financiar, regulamentul acoperă o serie de entități financiare reglementate la nivelul Uniunii, și anume instituțiile de credit, instituțiile de plată, instituțiile emitente de monedă electronică, firmele de investiții, furnizorii de servicii de criptoactive, depozitarii centrali de titluri de valoare, contrapărțile centrale, locurile de tranzacționare, registrele centrale de tranzacții, administratorii de fonduri de investiții alternative și de societăți de administrare, furnizorii de servicii de raportare a datelor, întreprinderile de asigurare și reasigurare, intermediarii de asigurări, intermediarii de reasigurări și intermediarii de asigurări auxiliare, instituțiile pentru furnizarea de pensii ocupaționale, agențiile de rating de credit, auditorii statutari și societățile de audit, administratorii indicilor de referință critici și furnizorii de servicii de finanțare participativă.

O astfel de acoperire facilitează aplicarea omogenă și coerentă a tuturor componentelor gestionării riscurilor în domeniile legate de TIC, garantând, în același timp, condiții de concurență echitabile în rândul entităților financiare în ceea ce privește obligațiile lor care recurg din reglementări cu privire la riscurile TIC. În același timp, regulamentul recunoaște că există diferențe semnificative între entitățile financiare din punctul de vedere al dimensiunii, al profilurilor comerciale sau al expunerii lor la riscul digital. Întrucât entitățile financiare mai mari dispun de mai multe resurse, doar entitățile financiare care nu se califică drept microîntreprinderi sunt obligate, de exemplu, să instituie mecanisme de guvernanță complexe, funcții de gestionare specifice, să efectueze evaluări aprofundate în urma unor schimbări majore în infrastructura rețelei și a sistemului informatic, să desfășoare periodic analize de risc privind sistemele TIC existente, să extindă testarea continuității activității și a planurilor de răspuns și de recuperare pentru a capta scenarii de transfer între infrastructura lor TIC primară și instalațiile redundante. În plus, numai entitățile financiare identificate ca fiind semnificative în scopul testării avansate a rezilienței digitale vor avea obligația de a efectua teste de penetrare bazate pe amenințări.

Fără a aduce atingere acestei acoperiri largi, aceasta nu este exhaustivă. În special, prezentul regulament nu surprinde operatorii de sistem definiți la articolul 2 litera (p) din Directiva 98/26/CE[22] privind caracterul definitiv al decontării în sistemele de plăți și de decontare a titlurilor de valoare și nici participanții la sistem, cu excepția cazului în care astfel de participanți sunt ei înșiși entități financiare reglementate la nivelul Uniunii și, ca atare, ar intra de drept în domeniul de aplicare al prezentului regulament (și anume instituții de credit, firme de investiții, CPC). În plus, registrul Uniunii pentru certificatele de emisii care

[22] Directiva 98/26/CE a Parlamentului European și a Consiliului din 19 mai 1998 privind caracterul definitiv al decontării în sistemele de plăți și de decontare a titlurilor de valoare (JO L 166, 11.6.1998, p. 45).

funcționează, în conformitate cu Directiva 2003/87/CE[23], sub egida Comisiei Europene se află, de asemenea, în afara domeniului de aplicare.

Aceste excluderi din Directiva privind caracterul definitiv al decontării țin seama de necesitatea unei noi revizuiri a aspectelor juridice și de politică care afectează operatorii de sisteme și participanți vizați de această directivă, luând în considerare în mod corespunzător impactul cadrelor care se aplică în prezent sistemelor de plată[24] gestionate de băncile centrale. Întrucât aceste chestiuni pot implica aspecte care rămân distincte de cele vizate de prezentul regulament, Comisia va continua să evalueze necesitatea și impactul unei noi extinderi a domeniului de aplicare al prezentului regulament la entitățile și infrastructurile TIC care nu se află, în prezent, în domeniul său de competență.

Cerințe legate de guvernanță (articolul 4)

Prezentul regulament urmărește o mai bună aliniere a strategiilor de afaceri ale entităților financiare și a modalității de gestionare a riscurilor TIC. În acest scop, organul de conducere va trebui să păstreze un rol esențial, activ, în coordonarea cadrului de gestionare a riscurilor TIC și să urmărească respectarea unei igiene cibernetice solide. Responsabilitatea deplină a organului de conducere în gestionarea riscurilor TIC aferente entității financiare va fi un principiu general care trebuie transpus în continuare într-o serie de cerințe specifice, cum ar fi alocarea unor roluri și responsabilități clare pentru toate funcțiile legate de TIC, un angajament continuu în ceea ce privește controlul monitorizării gestionării riscurilor TIC, precum și o gamă completă de procese de aprobare și de control și o alocare adecvată a investițiilor și cursurilor de formare în domeniul TIC.

Cerințe privind gestionarea riscurilor TIC (articolele 5-14)

Reziliența operațională digitală se bazează pe un set de principii și cerințe esențiale privind cadrul de gestionare a riscurilor TIC, în conformitate cu avizul tehnic comun al AES. Aceste cerințe, inspirate de standardele, orientările și recomandările relevante de la nivel internațional, național și sectorial, se articulează în jurul unor funcții specifice în gestionarea riscurilor TIC (identificare, protecție și prevenire, detectare, răspuns și recuperare, învățare și evoluție și comunicare). Pentru a ține pasul cu un peisaj în rapidă evoluție al amenințărilor cibernetice, entitățile financiare sunt obligate să instituie și să mențină sisteme și instrumente TIC reziliente, care să reducă la minimum impactul riscurilor TIC, să identifice în mod continuu toate sursele de riscuri TIC, să instituie măsuri de protecție și de prevenire, să detecteze prompt activitățile anormale, să pună în aplicare politici specifice și cuprinzătoare de continuitate a activității și planuri în caz de dezastru și planuri de recuperare ca parte integrantă a politicii operaționale de continuitate a activității. Componentele din urmă sunt necesare pentru o recuperare promptă după incidentele legate de TIC, în special atacuri cibernetice, prin limitarea daunelor și acordarea de prioritate reluării activităților în condiții de siguranță. Regulamentul nu impune, în sine, o standardizare specifică, ci se bazează mai degrabă pe standardele tehnice europene și cele recunoscute la nivel internațional sau pe cele mai bune practici din sector, în măsura în care acestea respectă pe deplin instrucțiunile de supraveghere privind utilizarea și integrarea unor astfel de standarde internaționale. Prezentul regulament acoperă, de asemenea, integritatea, siguranța și rezistența infrastructurilor și a

[23] Directiva 2003/87/CE a Parlamentului European și a Consiliului din 13 octombrie 2003 de stabilire a unui sistem de comercializare a cotelor de emisie de gaze cu efect de seră în cadrul Comunității și de modificare a Directivei 96/61/CE a Consiliului (JO L 275, 25.10.2003, p. 32).

[24] În special, Regulamentul (UE) nr. 795/2014 al Băncii Centrale Europene din 3 iulie 2014 privind cerințele de monitorizare pentru sistemele de plăți de importanță sistemică.

instalațiilor fizice care sprijină utilizarea tehnologiei și procesele TIC relevante, precum și persoanele implicate în acestea, ca parte a amprentei digitale a operațiunilor unei entități financiare.

Raportarea incidentelor legate de TIC (articolele 15-20)

Armonizarea și simplificarea raportării incidentelor legate de TIC se realizează, în primul rând, printr-o cerință generală ca entitățile financiare să stabilească și să pună în aplicare un proces de gestionare pentru a monitoriza și a înregistra incidentele legate de TIC, urmată de obligația de a le clasifica pe baza unor criterii detaliate în regulament și dezvoltate în continuare de AES pentru a specifica pragurile de semnificație. În al doilea rând, numai incidentele legate de TIC care sunt considerate majore trebuie să fie raportate autorităților competente. Raportarea ar trebui să fie efectuată utilizând un model comun și urmând o procedură armonizată, elaborată de AES. Entitățile financiare trebuie să prezinte rapoarte inițiale, intermediare și finale și să își informeze utilizatorii și clienții, în cazul în care incidentul are sau poate avea un impact asupra intereselor lor financiare. Autoritățile competente ar trebui să transmită detalii pertinente privind incidentele către alte instituții sau autorități: AES, BCE și punctelor unice de contact desemnate în Directiva (UE) 2016/1148.

Pentru a demara un dialog între entitățile financiare și autoritățile competente care ar contribui la reducerea la minimum a impactului și la identificarea unor măsuri reparatorii adecvate, raportarea incidentelor majore legate de TIC ar trebui să fie completată de feedback și orientări în materie de supraveghere.

În cele din urmă, posibilitatea de centralizare la nivelul Uniunii a rapoartelor privind incidentele legate de TIC ar trebui analizată în continuare într-un raport comun al AES, BCE și ENISA, în care să fie evaluată fezabilitatea creării unei platforme UE unice pentru raportarea incidentelor majore legate de TIC de către entitățile financiare.

Testarea rezilienței operaționale digitale (articolele 21-24)

Capacitățile și funcțiile incluse în cadrul de gestionare a riscurilor TIC trebuie să fie testate periodic din punctul de vedere al pregătirii și identificării punctelor slabe, a deficiențelor sau a lacunelor, precum și al punerii rapide în aplicare a măsurilor corective. Prezentul regulament permite aplicarea proporțională a cerințelor privind testarea rezilienței operaționale digitale, în funcție de dimensiunea și de profilul de afaceri și de risc ale entităților financiare: deși toate entitățile ar trebui să efectueze o testare a instrumentelor și sistemelor TIC, numai cele identificate de autoritățile competente (pe baza criteriilor din prezentul regulament și dezvoltate în continuare de AES) ca fiind semnificative și mature din punct de vedere cibernetic ar trebui să fie obligate să efectueze testări avansate prin teste de penetrare bazate pe amenințări (*threat led penetration test* – TLPT). Prezentul regulament stabilește, de asemenea, cerințe pentru entitățile care efectuează testele și pentru recunoașterea rezultatelor testelor TLPT în Uniune în cazul entităților financiare care își desfășoară activitatea în mai multe state membre.

Riscurile TIC generate de părți terțe (articolele 25-39)

Regulamentul are scopul de a asigura o monitorizare solidă a riscurilor TIC generate de părți terțe. Acest obiectiv va fi atins în primul rând prin respectarea normelor bazate pe principii care se aplică în cazul monitorizării, de către entitățile financiare, a riscurilor generate de furnizorii terți de servicii TIC. În al doilea rând, prezentul regulament armonizează elementele-cheie ale serviciului și ale relației cu furnizorii terți de servicii TIC. Aceste elemente acoperă aspecte minime considerate esențiale pentru a permite o monitorizare completă de către entitatea financiară a riscurilor TIC generate de părți terțe pe durata etapelor de încheiere, executare, încetare și a celor post-contractuale ale relației lor.

În special, contractele care reglementează relația respectivă vor trebui să conțină o descriere completă a serviciilor, indicarea locurilor în care urmează să fie prelucrate datele, descrieri complete ale nivelului de servicii, însoțite de obiective cantitative și calitative de performanță, dispoziții relevante privind accesibilitatea, disponibilitatea, integritatea, securitatea și protecția datelor cu caracter personal, precum și garanții de acces, recuperare și returnare în cazul unor disfuncționalități ale furnizorilor terți de servicii TIC, perioade de preaviz și obligații de raportare ale furnizorilor terți de servicii TIC, drepturi de acces, inspecție și audit pentru entitatea financiară sau o parte terță desemnată, drepturi clare de reziliere și strategii de ieșire dedicate. În plus, întrucât unele dintre aceste elemente contractuale pot fi standardizate, regulamentul promovează utilizarea voluntară a clauzelor contractuale standard care urmează să fie elaborate pentru utilizarea de către Comisie a serviciului de cloud computing.

În cele din urmă, regulamentul urmărește să promoveze convergența abordărilor în materie de supraveghere a riscurilor TIC generate de părți terțe în sectorul financiar, prin includerea furnizorilor terți esențiali de servicii TIC într-un cadru de supraveghere al Uniunii. Printr-un nou cadru legislativ armonizat, AES desemnată în calitate de supraveghetor principal pentru fiecare astfel de furnizor terț esențial de servicii TIC primește competențe pentru a asigura că furnizorii de servicii tehnologice care îndeplinesc un rol esențial pentru funcționarea sectorului financiar sunt monitorizați în mod adecvat la scară paneuropeană. Cadrul de supraveghere avut în vedere de prezentul regulament se bazează pe arhitectura instituțională existentă în domeniul serviciilor financiare, în care Comitetul comun al AES asigură coordonarea transsectorială în ceea ce privește toate aspectele legate de riscurile TIC, în conformitate cu sarcinile care îi revin în materie de securitate cibernetică, cu sprijinul subcomitetului relevant (Forumul de supraveghere) care desfășoară activități pregătitoare pentru decizii individuale și recomandări colective pentru furnizorii terți esențiali.

Schimbul de informații (articolul 40)

Pentru a crește gradul de sensibilizare cu privire la riscurile TIC, a reduce la minimum răspândirea acestora, a sprijini capabilitățile de apărare ale entităților financiare și tehnicile de detectare a amenințărilor, regulamentul permite entităților financiare să instituie mecanisme pentru a face schimb între ele de informații și date operative privind amenințările cibernetice.

2020/0266 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014 și (UE) nr. 909/2014

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

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

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Băncii Centrale Europene[25],

având în vedere avizul Comitetului Economic și Social European[26],

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) În era digitală, tehnologia informației și a comunicațiilor (TIC) sprijină sistemele complexe utilizate pentru activitățile de zi cu zi ale societății. Aceasta susține activitatea economiilor noastre în sectoare-cheie, inclusiv în cel financiar, și îmbunătățește funcționarea pieței unice. Creșterea gradului de digitalizare și de interconectare amplifică, de asemenea, riscurile TIC, ceea ce face ca societatea în ansamblu – și sistemul financiar, în special – să fie mai vulnerabilă la amenințările cibernetice sau la perturbările din domeniul TIC. Deși utilizarea omniprezentă a sistemelor TIC și gradul ridicat de digitalizare și conectivitate sunt în prezent caracteristicile de bază ale tuturor activităților entităților financiare din Uniune, reziliența digitală nu este încă suficient de solidă în cadrele lor operaționale.

(2) În ultimele decenii, utilizarea TIC a dobândit un rol esențial în domeniul finanțelor, având în prezent o relevanță critică în ceea ce privește operarea funcțiilor zilnice tipice ale tuturor entităților financiare. Digitalizarea acoperă, de exemplu, plățile, care au trecut tot mai mult de la metodele bazate pe numerar și pe suportul de hârtie la utilizarea soluțiilor digitale, precum și compensarea și decontarea titlurilor de valoare, tranzacționarea electronică și algoritmică, operațiunile de creditare și de finanțare, finanțarea *inter pares*, ratingul de credit, subscrierea asigurărilor, gestionarea creanțelor și operațiunile de tip *back-office*. Finanțele nu numai că au devenit în mare parte digitale în întregul sector, însă digitalizarea a aprofundat, de asemenea, interconexiunile și dependențele din cadrul sectorului financiar, precum și cu furnizorii terți de infrastructură și servicii.

[25] [*se adaugă trimiterea*] JO C , , p. .
[26] [*se adaugă trimiterea*] JO C , , p. .

(3) Comitetul european pentru risc sistemic (CERS) a reafirmat într-un raport din 2020 care abordează riscul cibernetic sistemic[27] modul în care nivelul ridicat existent de interconectare între entitățile financiare, piețele financiare și infrastructurile pieței financiare și, în special, interdependențele dintre sistemele lor TIC pot constitui o vulnerabilitate sistemică, întrucât incidentele cibernetice localizate s-ar putea răspândi rapid de la oricare dintre cele aproximativ 22 000 de entități financiare ale Uniunii[28] la întregul sistem financiar, nestingherite de limitele geografice. Breșele grave de securitate a TIC, care au loc în domeniul finanțelor, nu afectează doar entitățile financiare luate separat. Acestea facilitează, de asemenea, propagarea vulnerabilităților localizate la nivelul canalelor de transmisie financiară și pot avea consecințe negative asupra stabilității sistemului financiar al Uniunii, generând retrageri masive de lichiditate și o pierdere generală a încrederii în piețele financiare.

(4) În ultimii ani, riscurile TIC au atras atenția responsabililor de elaborarea politicilor, a organismelor de reglementare și a organismelor de standardizare de la nivel național, european și internațional într-o încercare de a spori reziliența, a stabili standarde și a coordona activitatea de reglementare sau de supraveghere. La nivel internațional, Comitetul de la Basel pentru supraveghere bancară, Comitetul pentru infrastructuri de plăți și de piață, Consiliul pentru Stabilitate Financiară, Institutul pentru Stabilitate Financiară, precum și grupurile de țări G7 și G20 urmăresc să furnizeze autorităților competente și operatorilor pe piață din diferite jurisdicții instrumente care să consolideze reziliența sistemelor lor financiare.

(5) În pofida inițiativelor specifice de politică și legislative naționale și europene, riscurile TIC reprezintă în continuare o provocare la adresa rezilienței operaționale, a performanței și a stabilității sistemului financiar al Uniunii. Reforma care a urmat crizei financiare din 2008 a consolidat în primul rând reziliența financiară a sectorului financiar al Uniunii și a vizat protejarea competitivității Uniunii și a stabilității din punct de vedere economic, prudențial și al conduitei pe piață. Deși securitatea TIC și reziliența digitală fac parte din riscul operațional, acestea s-au aflat mai puțin în centrul agendei de reglementare post-criză și s-au fost dezvoltat doar în unele domenii ale politicii și ale cadrului de reglementare al serviciilor financiare din Uniune sau numai în câteva state membre.

(6) Planul de acțiune al Comisiei din 2018 privind FinTech[29] a evidențiat importanța capitală a creșterii rezilienței sectorului financiar al Uniunii și din punct de vedere operațional, pentru a asigura siguranța tehnologică și buna sa funcționare, recuperarea rapidă în urma unor breșe și a incidentelor legate de TIC, permițând în cele din urmă

---

27 Raportul CERS privind riscurile cibernetice sistemice, februarie 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

28 Potrivit evaluării impactului care însoțește analiza autorităților europene de supraveghere, [SWD(2017)308], există aproximativ 5 665 de instituții de credit, 5 934 de firme de investiții, 2 666 de întreprinderi de asigurare, 1 573 IORP, 2 500 de societăți de administrare a investițiilor, 350 de infrastructuri ale pieței (precum CPC, burse de valori, operatori independenți, registre centrale de tranzacții și sisteme multilaterale de tranzacționare), 45 de agenții de rating de credit și 2 500 de instituții de plată autorizate și instituții emitente de monedă electronică. Suma se ridică până la aproximativ 21 233 de entități și nu include entități de finanțare participativă, auditori statutari și societățile de audit, furnizori de servicii bazate pe criptoactive și administratori de indici de referință.

29 Comunicarea Comisiei către Parlamentul European, Consiliu, Banca Centrală Europeană, Comitetul Economic și Social European și Comitetul Regiunilor, *Planul de acțiune privind FinTech: pentru un sector financiar european mai competitiv și mai inovator*, COM/2018/0109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.

furnizarea efectivă și fără sincope a serviciilor financiare în întreaga Uniune, inclusiv în situații de criză, și menținând totodată încrederea consumatorilor și a pieței.

(7) În aprilie 2019, Autoritatea Bancară Europeană (ABE), Autoritatea Europeană pentru Valori Mobiliare și Piețe (ESMA) și Autoritatea Europeană de Asigurări și Pensii Ocupaționale (EIOPA) (denumite în comun „autoritățile europene de supraveghere” sau „AES”) au emis în comun două avize tehnice prin care solicită o abordare coerentă a riscurilor TIC în domeniul finanțelor și recomandă consolidarea, în mod proporțional, a rezilienței operaționale digitale a sectorului serviciilor financiare printr-o inițiativă sectorială a Uniunii.

(8) Sectorul financiar al Uniunii este reglementat printr-un cadru unic de reglementare armonizat și este guvernat de un sistem european de supraveghere financiară. Cu toate acestea, dispozițiile privind reziliența operațională digitală și securitatea TIC nu sunt încă armonizate pe deplin sau în mod consecvent, în pofida faptului că reziliența operațională digitală este vitală pentru asigurarea stabilității financiare și a integrității pieței în era digitală și nu este mai puțin importantă decât, de exemplu, standardele comune prudențiale sau de conduită pe piață. Prin urmare, cadrul unic de reglementare și sistemul de supraveghere ar trebui să fie dezvoltate pentru a acoperi și această componentă, prin extinderea mandatelor autorităților de supraveghere financiară însărcinate cu monitorizarea și protejarea stabilității financiare și a integrității pieței.

(9) Disparitățile legislative și abordările naționale inegale în materie de reglementare sau de supraveghere cu privire la riscurile TIC determină obstacole în calea pieței unice a serviciilor financiare, împiedicând exercitarea fără sincope a libertății de stabilire și de prestare de servicii pentru entitățile financiare cu o prezență transfrontalieră. Concurența între entități financiare de același tip care operează în diferite state membre poate, de asemenea, să fie denaturată. În special, pentru domeniile în care armonizarea la nivelul Uniunii a fost foarte limitată până în prezent – precum testarea rezilienței operaționale digitale – sau absentă – de exemplu, monitorizarea riscurilor TIC generate de părți terțe – disparitățile care derivă din evoluțiile preconizate la nivel național ar putea genera noi obstacole în calea funcționării pieței unice, în detrimentul participanților la piață și al stabilității financiare.

(10) Modul parțial în care dispozițiile privind riscurile TIC au fost abordate până în prezent la nivelul Uniunii prezintă lacune sau suprapuneri în domenii importante, cum ar fi raportarea incidentelor legate de TIC și testarea rezilienței operaționale digitale, și creează inconsecvențe ca urmare a apariției unor norme naționale divergente sau a aplicării ineficiente din punctul de vedere al costurilor a unor norme care se suprapun. Acest lucru este în special în detrimentul domeniilor care utilizează intensiv TIC, precum finanțele, deoarece riscurile legate de tehnologie nu au frontiere, iar sectorul financiar își desfășoară serviciile pe o bază transfrontalieră largă, în interiorul și în afara Uniunii.

Entitățile financiare individuale care desfășoară activități transfrontaliere sau dețin mai multe autorizații (de exemplu, o entitate financiară poate avea o autorizație bancară, o autorizație de firmă de investiții și o autorizație de instituție de plată, fiecare dintre aceste autorizații fiind emisă de o altă autoritate competentă din unul sau mai multe state membre) se confruntă cu provocări operaționale în ceea ce privește abordarea riscurilor TIC și atenuarea efectelor adverse ale incidentelor TIC pe cont propriu și într-un mod coerent și eficient din punctul de vedere al costurilor.

(11) Întrucât cadrul unic de reglementare nu a fost însoțit de un cadru cuprinzător privind riscurile TIC sau riscurile operaționale, este necesară armonizarea în continuare a

principalelor cerințe privind reziliența operațională digitală a tuturor entităților financiare. Capacitățile și reziliența generală pe care entitățile financiare, pe baza unor astfel de cerințe principale, le-ar dezvolta pentru a rezista întreruperilor operaționale, ar contribui la menținerea stabilității și integrității piețelor financiare ale Uniunii și, astfel, la asigurarea unui nivel ridicat de protecție pentru investitorii și consumatorii din Uniune. Întrucât urmărește să contribuie la buna funcționare a pieței unice, prezentul regulament ar trebui să se bazeze pe dispozițiile articolului 114 din TFUE, astfel cum au fost interpretate în conformitate cu jurisprudența constantă a Curții de Justiție a Uniunii Europene.

(12) Prezentul regulament urmărește, în primul rând, să consolideze și să actualizeze cerințele privind riscurile TIC abordate până în prezent în mod separat în diferitele regulamente și directive. Deși au acoperit principalele categorii de riscuri financiare (de exemplu, riscul de credit, riscul de piață, riscul de credit al contrapărții și riscul de lichiditate, riscul de conduită pe piață), actele juridice respective ale Uniunii nu au putut aborda în mod cuprinzător, la momentul adoptării lor, toate componentele rezilienței operaționale. Atunci când au fost dezvoltate în continuare în aceste acte juridice ale Uniunii, cerințele privind riscul operațional au favorizat, adesea, o abordare cantitativă tradițională a riscurilor (și anume, stabilirea unei cerințe de capital pentru a acoperi riscurile TIC), mai degrabă decât consacrarea unor cerințe calitative specifice pentru a stimula capacitățile prin cerințe care vizau capacitățile de protecție, detectare, limitare, recuperare și reparare în raport cu incidentele legate de TIC sau prin stabilirea unor capacități de raportare și testare digitală. Directivele și regulamentele respective au vizat, în principal, să acopere norme esențiale privind supravegherea prudențială, integritatea pieței sau conduita pe piață.

Prin prezentul exercițiu de consolidare și actualizare a normelor privind riscurile TIC, toate dispozițiile care abordează riscul digital în domeniul finanțelor ar fi reunite pentru prima dată, într-un mod coerent, într-un singur act legislativ. Această inițiativă ar trebui să elimine astfel lacunele sau inconsecvențele la nivelul remedierii din unele dintre aceste acte juridice, inclusiv în ceea ce privește terminologia utilizată în acestea, și ar trebui să facă trimiteri explicite la riscurile TIC prin intermediul unor norme specifice privind capacitățile de gestionare a riscurilor TIC, raportarea și testarea și monitorizarea riscurilor generate de părți terțe.

(13) Entitățile financiare ar trebui să urmeze aceeași abordare și să aceleași norme bazate pe principii atunci când abordează riscurile TIC. Consecvența contribuie la creșterea încrederii în sistemul financiar și la menținerea stabilității acestuia, în special în perioade de utilizare excesivă a sistemelor, a platformelor și a infrastructurilor TIC, ceea ce implică un risc digital sporit.

Respectarea unei igiene cibernetice de bază ar trebui, de asemenea, să permită evitarea impunerii unor costuri semnificative asupra economiei, prin reducerea la minimum a impactului și a costurilor asociate perturbărilor TIC.

(14) Utilizarea unui regulament ajută la reducerea complexității reglementării, favorizează convergența supravegherii, sporește securitatea juridică, contribuind totodată la limitarea costurilor de conformitate, în special pentru entitățile financiare care desfășoară activități transfrontaliere, precum și la reducerea denaturărilor concurenței. Alegerea unui regulament pentru instituirea unui cadru comun pentru reziliența operațională digitală a entităților financiare pare, prin urmare, să fie cel mai adecvat mod de a garanta o aplicare omogenă și coerentă a tuturor componentelor gestionării riscurilor TIC de către sectoarele financiare ale Uniunii.

(15) Pe lângă legislația privind serviciile financiare, Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului[30] reprezintă actualul cadru general de securitate cibernetică la nivelul Uniunii. Pe lângă cele șapte sectoare critice, directiva respectivă acoperă, de asemenea, trei tipuri de entități financiare, și anume instituțiile de credit, locurile de tranzacționare și contrapărțile centrale. Totuși, întrucât Directiva (UE) 2016/1148 stabilește un mecanism de identificare la nivel național a operatorilor de servicii esențiale, doar anumite instituții de credit, locuri de tranzacționare și contrapărți centrale identificate de statele membre sunt, în practică, incluse în domeniul său de aplicare și, prin urmare, trebuie să respecte cerințele privind securitatea TIC și notificarea incidentelor prevăzute în aceasta.

(16) Întrucât ridică nivelul de armonizare în ceea ce privește componentele rezilienței digitale, prin introducerea unor cerințe privind gestionarea riscurilor TIC și raportarea incidentelor legate de TIC care sunt mai stricte comparativ cu cele prevăzute în legislația actuală a Uniunii privind serviciile financiare, prezentul regulament constituie o armonizare sporită, de asemenea, în raport cu cerințele prevăzute în Directiva (UE) 2016/1148. Prin urmare, prezentul regulament constituie o *lex specialis* la Directiva (UE) 2016/1148.

Este esențial să se mențină o relație puternică între sectorul financiar și cadrul orizontal de securitate cibernetică al Uniunii, care să asigure coerența cu strategiile de securitate cibernetică deja adoptate de statele membre și să permită ca autoritățile de supraveghere financiară să fie sensibilizate cu privire la incidentele cibernetice care afectează alte sectoare vizate de Directiva (UE) 2016/1148.

(17) Pentru a permite un proces de învățare transsectorial și pentru a valorifica în mod eficace experiențele altor sectoare în ceea ce privește abordarea amenințărilor cibernetice, entitățile financiare menționate în Directiva (UE) 2016/1148 ar trebui să facă în continuare parte din „ecosistemul” directivei respective (de exemplu, Grupul de cooperare NIS și CSIRT).

AES și, respectiv, autoritățile naționale competente ar trebui să poată participa la discuțiile de politică strategice și la lucrările tehnice ale Grupului de cooperare NIS, respectiv, la schimburi de informații, precum și să coopereze în continuare cu punctele unice de contact desemnate în Directiva (UE) 2016/1148. Autoritățile competente în temeiul prezentului regulament ar trebui, de asemenea, să consulte și să coopereze cu CSIRT naționale desemnate în conformitate cu articolul 9 din Directiva (UE) 2016/1148.

(18) Este, de asemenea, important să se asigure consecvența cu Directiva privind infrastructura critică europeană (ICE), care este în prezent în curs de revizuire, pentru a spori protecția și reziliența infrastructurilor critice împotriva amenințărilor care nu sunt legate de domeniul cibernetic, cu posibile implicații pentru sectorul financiar[31].

(19) Furnizorii de servicii de cloud computing sunt o categorie de furnizori de servicii digitale care intră sub incidența Directivei (UE) 2016/1148. Ca atare, aceștia fac obiectul supravegherii *ex post* de către autoritățile naționale desemnate în conformitate

---

30 Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (JO L 194, 19.7.2016, p. 1).

31 Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora (JO L 345, 23.12.2008, p. 75).

cu directiva menționată, care se limitează la cerințele privind securitatea TIC și notificarea incidentelor prevăzute în actul respectiv. Întrucât se aplică tuturor furnizorilor terți esențiali de servicii TIC, inclusiv furnizorilor de servicii de cloud computing atunci când furnizează servicii TIC entităților financiare, cadrul de supraveghere instituit prin prezentul regulament ar trebui să fie considerat complementar supravegherii care are loc în temeiul Directivei (UE) 2016/1148. În plus, cadrul de supraveghere instituit prin prezentul regulament ar trebui să acopere furnizorii de servicii de cloud computing, în absența unui cadru orizontal al Uniunii care să nu fie specializat pe anumite sectoare și care să instituie o Autoritate de supraveghere digitală.

(20) Pentru a păstra controlul deplin asupra riscurilor TIC, entitățile financiare trebuie să dispună de capacități cuprinzătoare care să permită o gestionare puternică și eficace a riscurilor TIC, alături de mecanisme și politici specifice pentru raportarea incidentelor legate de TIC, testarea sistemelor, a controalelor și a proceselor TIC, precum și gestionarea riscurilor TIC generate de părți terțe. Nivelul de reziliență operațională digitală pentru sistemul financiar ar trebui ridicat, permițând, în același timp, aplicarea proporțională a cerințelor pentru entitățile financiare care sunt microîntreprinderi, astfel cum sunt definite în Recomandarea 2003/361/CE a Comisiei[32].

(21) Pragurile de raportare a incidentelor legate de TIC și taxonomiile variază semnificativ la nivel național. Deși un numitor comun poate fi atins prin intermediul activităților relevante întreprinse de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)[33] și de Grupul de cooperare NIS pentru entitățile financiare vizate de Directiva (UE) 2016/1148, abordările divergente privind pragurile și taxonomiile încă există sau pot apărea pentru restul entităților financiare. Aceasta implică cerințe multiple pe care entitățile financiare trebuie să le respecte, în special atunci când își desfășoară activitatea în mai multe jurisdicții ale Uniunii și când fac parte dintr-un grup financiar. În plus, aceste divergențe pot împiedica crearea unor noi mecanisme uniforme sau centralizate la nivelul Uniunii, care să accelereze procesul de raportare și să sprijine un schimb de informații rapid și fără sincope între autoritățile competente, care este esențial pentru abordarea riscurilor TIC în cazul unor atacuri la scară largă cu consecințe potențial sistemice.

(22) Pentru a permite autorităților competente să își îndeplinească rolurile de supraveghere prin obținerea unei imagini de ansamblu complete asupra naturii, frecvenței, importanței și impactului incidentelor legate de TIC și pentru a intensifica schimbul de informații între autoritățile publice relevante, inclusiv autoritățile de aplicare a legii și autoritățile de rezoluție, este necesar să se stabilească norme pentru completarea regimului de raportare a incidentelor legate de TIC cu cerințele care lipsesc în prezent din legislația privind subsectorul financiar și să se elimine orice suprapuneri și dublări existente, pentru a atenua costurile. Prin urmare, este esențial să se armonizeze regimul de raportare a incidentelor legate de TIC prin impunerea obligației ca toate entitățile financiare să raporteze numai autorităților lor competente. În plus, AES ar trebui să fie împuternicite să specifice în continuare elementele aferente raportării incidentelor

---

32 Recomandarea Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii (JO L 124, 20.5.2003, p. 36).

33 ENISA Reference Incident Classification Taxonomy, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

legate de TIC, cum ar fi taxonomia, intervalele de timp, seturile de date, modelele și pragurile aplicabile.

(23) Cerințele privind testarea rezilienței operaționale digitale s-au dezvoltat în unele subsectoare financiare în mai multe cadre naționale necoordonate, care abordează aceleași aspecte într-un mod diferit. Aceasta conduce la dublarea costurilor pentru entitățile financiare transfrontaliere și îngreunează recunoașterea reciprocă a rezultatelor. Testarea necoordonată poate, așadar, să segmenteze piața unică.

(24) În plus, în cazurile în care nu este necesară testarea, vulnerabilitățile rămân nedetectate, ceea ce expune entitatea financiară și, în cele din urmă, stabilitatea și integritatea sectorului financiar unui risc mai ridicat. Fără intervenția Uniunii, testarea rezilienței operaționale digitale ar continua să fie neuniformă și nu ar exista o recunoaștere reciprocă a rezultatelor testelor între diferite jurisdicții. De asemenea, întrucât este puțin probabil ca alte subsectoare financiare să adopte astfel de sisteme la o scară semnificativă, acestea nu s-ar bucura de beneficiile potențiale, de exemplu dezvăluirea vulnerabilităților și a riscurilor, testarea capabilităților de apărare și a continuității activității, precum și creșterea încrederii consumatorilor, a furnizorilor și a partenerilor de afaceri. Pentru a remedia astfel de suprapuneri, divergențe și lacune, este necesar să se stabilească norme care să vizeze testarea coordonată de către entitățile financiare și autoritățile competente, facilitând astfel recunoașterea reciprocă a testelor avansate pentru entitățile financiare semnificative.

(25) Dependența entităților financiare de serviciile TIC este determinată parțial de nevoia lor de a se adapta la o economie globală digitală competitivă emergentă, de a spori eficiența activității lor și de a răspunde cererii consumatorilor. Natura și amploarea unei astfel de dependențe a fost în continuă evoluție în ultimii ani, conducând la o reducere a costurilor în cadrul intermedierii financiare, permițând dezvoltarea și scalabilitatea activităților financiare și oferind în același timp o gamă largă de instrumente TIC pentru gestionarea proceselor interne complexe.

(26) Această utilizare extinsă a serviciilor TIC este demonstrată de acorduri contractuale complexe, din cauza cărora entitățile financiare se confruntă adesea cu dificultăți în negocierea unor condiții contractuale care să fie adaptate la standardele prudențiale sau la alte cerințe de reglementare pe care trebuie să le respecte, sau, altfel, în exercitarea unor drepturi specifice, cum ar fi drepturile de acces sau de audit, atunci când acestea din urmă sunt consacrate în acorduri. În plus, multe astfel de contracte nu oferă garanții suficiente care să permită o monitorizare completă a proceselor de subcontractare, privând astfel entitatea financiară de capacitatea sa de a evalua aceste riscuri asociate. În plus, întrucât furnizorii terți de servicii TIC oferă adesea servicii standardizate diferitelor tipuri de clienți, astfel de contracte nu răspund întotdeauna în mod adecvat nevoilor individuale sau specifice ale actorilor din sectorul financiar.

(27) În pofida unor norme generale privind externalizarea în unele dintre actele legislative ale Uniunii din domeniul serviciilor financiare, monitorizarea dimensiunii contractuale nu este pe deplin ancorată în legislația Uniunii. În absența unor standarde ale Uniunii clare și specifice care să se aplice acordurilor contractuale încheiate cu furnizorii terți de servicii TIC, sursa externă a riscurilor TIC nu este abordată în mod cuprinzător. Prin urmare, este necesar să se stabilească anumite principii-cheie care să orienteze gestionarea de către entitățile financiare a riscurilor TIC generate de părți terțe, însoțite de un set de drepturi contractuale de bază în legătură cu mai multe elemente ale executării și rezilierii contractelor, astfel încât să consacre anumite garanții minime

care să stea la baza capacității entităților financiare de a monitoriza în mod eficace toate riscurile care apar la nivelul părților terțe care furnizează servicii TIC.

(28) Există o lipsă de omogenitate și de convergență în ceea ce privește riscurile TIC generate de părți terțe și dependențele de serviciile TIC furnizate de părți terțe. În pofida unor eforturi de abordare a domeniului specific al externalizării, precum recomandările din 2017 privind externalizarea către furnizorii de servicii de tip cloud[34], aspectul riscului sistemic care poate fi declanșat de expunerea sectorului financiar la un număr limitat de furnizori terți esențiali de servicii TIC este foarte puțin abordată în legislația Uniunii. Această lipsă la nivelul Uniunii este agravată de absența unor mandate și instrumente specifice care să permită autorităților naționale de supraveghere să dobândească o bună înțelegere a dependențelor de servicii TIC furnizate de părți terțe și să monitorizeze în mod adecvat riscurile care decurg din concentrarea acestor dependențe de servicii TIC furnizate de părți terțe.

(29) Ținând seama de riscurile sistemice potențiale implicate de practicile de externalizare sporite și de concentrarea serviciilor TIC furnizate de părți terțe și având în vedere insuficiența mecanismelor naționale care permit autorităților de supraveghere financiară cuantificarea, calificarea și remedierea consecințelor riscurilor TIC care apar la nivelul furnizorilor terți esențiali de servicii TIC, este necesar să se instituie un cadru adecvat de supraveghere la nivelul Uniunii, care să permită monitorizarea continuă a activităților furnizorilor terți de servicii TIC care sunt furnizori esențiali pentru entitățile financiare.

(30) Întrucât amenințările TIC devin tot mai complexe și sofisticate, măsurile eficiente de detectare și de prevenire depind în mare măsură de schimbul periodic de date operative privind amenințările și vulnerabilitatea între entitățile financiare. Schimbul de informații contribuie la creșterea gradului de sensibilizare cu privire la amenințările cibernetice, care, la rândul său, consolidează capacitatea entităților financiare de a preveni materializarea amenințărilor în incidente reale și permite entităților financiare să limiteze mai bine efectele incidentelor legate de TIC și să se redreseze mai eficient. În absența unor orientări la nivelul Uniunii, mai mulți factori par să fi împiedicat astfel de schimburi de date operative, în special incertitudinea cu privire la compatibilitatea cu normele privind protecția datelor, a normelor antitrust și a celor privind răspunderea.

(31) În plus, ezitările cu privire la tipul de informații care pot fi partajate cu alți participanți pe piață sau cu autorități care nu au funcții de supraveghere (precum ENISA, pentru contribuții analitice sau Europol, în scopul aplicării legii) conduc la reținerea unor informații utile. Amploarea și calitatea schimbului de informații rămân limitate, fragmentate, schimburile relevante fiind realizate în cea mai mare parte la nivel local (prin inițiative naționale) și fără acorduri consecvente de schimb de informații la nivelul Uniunii, adaptate nevoilor unui sector financiar integrat.

(32) Entitățile financiare ar trebui, prin urmare, să fie încurajate să își valorifice în mod colectiv cunoștințele individuale și experiența practică la nivel strategic, tactic și operațional, pentru a-și consolida capacitățile de evaluare, de monitorizare, de apărare și de răspuns în mod adecvat la amenințările cibernetice. Prin urmare, este necesar să se favorizeze apariția la nivelul Uniunii a unor mecanisme pentru acorduri voluntare de schimb de informații care, atunci când au loc în medii de încredere, ar ajuta

[34] Recomandări privind externalizarea către furnizori de servicii de tip cloud (EBA/REC/2017/03), în prezent abrogate de Ghidul ABE privind externalizarea (EBA/GL/2019/02).

comunitatea financiară să prevină ameninţările şi să răspundă în mod colectiv la acestea prin limitarea rapidă a răspândirii riscurilor TIC şi prin împiedicarea unei contaminări potenţiale pe toate canalele financiare. Aceste mecanisme ar trebui aplicate cu respectarea deplină a normelor Uniunii aplicabile în domeniul concurenţei[35], precum şi într-un mod care să garanteze respectarea deplină a normelor Uniunii privind protecţia datelor, în special Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului[36], îndeosebi în contextul prelucrării datelor cu caracter personal care este necesară în scopul interesului legitim urmărit de operator sau de o parte terţă, astfel cum se menţionează la articolul 6 alineatul (1) litera (f) din regulamentul respectiv.

(33) În pofida acoperirii largi prevăzute de prezentul regulament, aplicarea normelor privind reziliența operațională digitală ar trebui să țină seama de diferențele semnificative dintre entitățile financiare din punctul de vedere al dimensiunii, al profilurilor de afaceri sau al expunerii la riscul digital. Ca principiu general, atunci când se direcționează resurse și capacități către punerea în aplicare a cadrului de gestionare a riscurilor TIC, entitățile financiare ar trebui să își echilibreze în mod corespunzător nevoile în materie de TIC în funcție de dimensiunea și profilul lor de afaceri, în timp ce autoritățile competente ar trebui să continue să evalueze și să revizuiască abordarea acestei distribuiri.

(34) Întrucât entitățile financiare mai mari se pot bucura de resurse mai ample și ar putea mobiliza rapid fonduri pentru a dezvolta structuri de guvernanță și a institui diverse strategii corporative, numai entitățile financiare care nu sunt microîntreprinderi în sensul prezentului regulament ar trebui să aibă obligația de a institui mecanisme de guvernanță mai complexe. Astfel de entități sunt mai bine echipate, în special, pentru a institui funcții de gestionare dedicate supravegherii acordurilor cu furnizorii terți de servicii TIC sau gestionării crizelor, pentru a-și organiza gestionarea riscurilor TIC în conformitate cu cele trei linii ale modelului de apărare sau pentru a adopta un document privind resursele umane, care să explice în mod cuprinzător politicile privind drepturile de acces.

În mod similar, numai acestor entități financiare ar trebui să li se solicite să efectueze evaluări aprofundate în urma unor schimbări majore în infrastructurile și procesele de rețea și ale sistemului informatic, să efectueze periodic analize ale riscului cu privire la sistemele TIC existente sau să extindă testarea planurilor privind continuitatea activității și a planurilor de răspuns și de recuperare pentru a capta scenariile de transfer între infrastructura TIC primară și instalațiile redundante.

(35) În plus, întrucât numai acele entități financiare care au fost identificate ca fiind semnificative în scopul testării avansate a rezilienței digitale ar trebui să aibă obligația de a efectua teste de penetrare bazate pe amenințări, procesele administrative și costurile financiare implicate de efectuarea unor astfel de teste ar trebui să fie transferate către un procent mic de entități financiare. În cele din urmă, în vederea reducerii sarcinilor de reglementare, doar entitățile financiare, altele decât microîntreprinderile, ar trebui să fie invitate să raporteze periodic autorităților

---

35 Comunicarea Comisiei – Orientări privind aplicabilitatea articolului 101 din Tratatul privind funcționarea Uniunii Europene acordurilor de cooperare orizontală, 2011/C 11/01.

36 Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

competente toate costurile și pierderile cauzate de perturbările TIC, precum și rezultatele analizelor post-incident în urma unor perturbări semnificative ale TIC.

(36) Pentru a asigura alinierea deplină și coerența globală între strategiile de afaceri ale entităților financiare, pe de o parte, și gestionarea riscurilor TIC, pe de altă parte, organul de conducere ar trebui să aibă obligația de a îndeplini un rol activ și esențial în orientarea și adaptarea cadrului de gestionare a riscurilor TIC și a strategiei globale privind reziliența digitală. Abordarea care urmează să fie adoptată de organul de conducere nu ar trebui să se concentreze numai pe mijloacele de asigurare a rezilienței sistemelor TIC, ci ar trebui să acopere, de asemenea, persoanele și procesele printr-un set de politici care cultivă, la fiecare nivel corporativ și pentru întregul personal, un sentiment puternic de conștientizare cu privire la riscurile cibernetice și un angajament de a respecta o igienă cibernetică strictă la toate nivelurile.

Cea din urmă responsabilitate a organului de conducere în gestionarea riscurilor TIC ale unei entități financiare ar trebui să constea într-un principiu general al acestei abordări cuprinzătoare, transpus în continuare în implicarea constantă a organului de conducere în monitorizarea gestionării riscurilor TIC.

(37) În plus, responsabilitatea deplină a organului de conducere merge mână în mână cu asigurarea unui nivel de investiții TIC și a unui buget general pentru ca entitatea financiară să poată atinge nivelul de referință al rezilienței operaționale digitale.

(38) Inspirat de standardele, orientările, recomandările sau abordările relevante de la nivel internațional, național și sectorial privind gestionarea riscului cibernetic[37], prezentul regulament promovează un set de funcții care facilitează structurarea globală a gestionării riscurilor TIC. Atât timp cât principalele capacități pe care entitățile financiare le instituie răspund nevoilor obiectivelor prevăzute de funcțiile (identificare, protecție și prevenire, detectare, răspuns și recuperare, învățare și evoluție și comunicare) stabilite în prezentul regulament, entitățile financiare au în continuare libertatea de a utiliza modele de gestionare a riscurilor TIC care sunt încadrate sau clasificate în mod diferit.

(39) Pentru a ține pasul cu un peisaj în evoluție al amenințărilor cibernetice, entitățile financiare ar trebui să mențină sisteme TIC actualizate, care să fie fiabile și dotate cu o capacitate suficientă nu numai pentru a garanta prelucrarea datelor, astfel cum este necesar pentru executarea serviciilor lor, ci și pentru a asigura reziliența tehnologică care să permită entităților financiare să trateze în mod adecvat nevoile de prelucrare suplimentare pe care condiții de criză a pieței sau alte situații nefavorabile le pot genera. Deși prezentul regulament nu implică nicio standardizare a unor sisteme, instrumente sau tehnologii TIC specifice, acesta se bazează pe utilizarea adecvată, de către entitățile financiare, a standardelor tehnice europene și recunoscute la nivel internațional (de exemplu, ISO) sau pe cele mai bune practici din sector, în măsura în care o astfel de utilizare este pe deplin conformă cu instrucțiunile de supraveghere specifice privind utilizarea și încorporarea standardelor internaționale.

---

[37] CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, https://www.bis.org/cpmi/publ/d146.pdf G7 *Fundamental Elements of Cybersecurity for the Financial Sector,* https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; NIST Cybersecurity Framework, https://www.nist.gov/cyberframework; FSB *CIRR toolkit*, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document.

(40) Sunt necesare planuri eficace privind continuitatea activității și recuperarea pentru a permite entităților financiare să soluționeze cu promptitudine și rapiditate incidentele legate de TIC, în special atacurile cibernetice, prin limitarea daunelor și acordând prioritate reluării activităților și a acțiunilor de recuperare. Totuși, deși sistemele de rezervă ar trebui să demareze prelucrarea fără întârzieri nejustificate, această demarare nu ar trebui în niciun caz să pună în pericol integritatea și securitatea rețelelor și a sistemelor informatice sau confidențialitatea datelor.

(41) Deși prezentul regulament permite entităților financiare să stabilească obiective privind durata recuperării într-un mod flexibil și, prin urmare, să stabilească astfel de obiective ținând seama pe deplin de natura și de importanța funcției relevante și de orice nevoi funcționale specifice, o evaluare a impactului global potențial asupra eficienței pieței ar trebui, de asemenea, să fie obligatorie atunci când se stabilesc astfel de obiective.

(42) Consecințele semnificative ale atacurilor cibernetice sunt amplificate atunci când apar în sectorul financiar, un domeniu mult mai expus riscului de a fi ținta propagatorilor rău-intenționați care urmăresc câștiguri financiare direct la sursă. Pentru a atenua astfel de riscuri și pentru a preveni pierderea integrității sistemelor TIC sau pierderea disponibilității acestora și încălcarea normelor privind confidențialitatea datelor sau prejudicierea infrastructurii TIC fizice, raportarea incidentelor majore legate de TIC de către entitățile financiare ar trebui să fie îmbunătățită în mod semnificativ.

Raportarea incidentelor legate de TIC ar trebui să fie armonizată pentru toate entitățile financiare, solicitându-se ca acestea să raporteze numai autorităților lor competente. Deși toate entitățile financiare ar face obiectul acestei raportări, nu toate ar trebui să fie afectate în același mod, deoarece pragurile de semnificație relevante și intervalele de timp ar trebui să fie calibrate pentru a capta numai incidentele majore legate de TIC. Raportarea directă ar permite autorităților de supraveghere financiară accesul la informații privind incidentele legate de TIC. Cu toate acestea, autoritățile de supraveghere financiară ar trebui să transmită aceste informații autorităților publice nefinanciare (autorităților competente din domeniul NIS, autorităților naționale de protecție a datelor și autorităților de aplicare a legii pentru incidente de natură penală). Informațiile referitoare la incidentele legate de TIC ar trebui transmise reciproc: autoritățile de supraveghere financiară ar trebui să furnizeze entității financiare tot feedbackul sau toate orientările necesare, în timp ce AES ar trebui să partajeze date anonimizate privind amenințările și vulnerabilitățile legate de un eveniment pentru a contribui la o apărare colectivă mai amplă.

(43) Ar trebui să se aibă în vedere o analiză suplimentară cu privire la posibila centralizare a rapoartelor privind incidentele legate de TIC, prin intermediul unei Platforme centrale unice a UE, fie prin primirea directă a rapoartelor relevante și notificarea automată a autorităților naționale competente, fie prin simpla centralizare a rapoartelor transmise de autoritățile naționale competente și îndeplinirea unui rol de coordonare. AES ar trebui să aibă obligația de a pregăti, în consultare cu BCE și ENISA, până la o anumită dată, un raport comun în care să analizeze fezabilitatea instituirii unei astfel de Platforme centrale a UE.

(44) Pentru a atinge o reziliență operațională digitală solidă și în conformitate cu standardele internaționale (de exemplu, elementele fundamentale ale G7 pentru testele de penetrare bazate pe amenințări), entitățile financiare ar trebui să își testeze în mod regulat sistemele și personalul din domeniul TIC cu privire la eficacitatea capacităților lor de prevenire, detectare, răspuns și recuperare, pentru a descoperi și a aborda

vulnerabilitățile potențiale în materie de TIC. Pentru a răspunde diferențelor dintre subsectoarele financiare și din cadrul acestora în ceea ce privește gradul de pregătire a entităților financiare în materie de securitate cibernetică, testarea ar trebui să includă o gamă variată de instrumente și acțiuni, de la o evaluare a cerințelor de bază (de exemplu, evaluări și examinări ale vulnerabilității, analize ale surselor deschise, evaluări ale securității rețelei, analize ale lacunelor, evaluări ale securității fizice, chestionare și soluții de scanare a programelor software, evaluări ale codului sursă, după caz, teste bazate pe scenarii, teste de compatibilitate, teste de performanță sau teste integrale) până la efectuarea unor teste mai avansate (de exemplu, teste TLPT pentru acele entități financiare suficient de mature din perspectiva TIC pentru a putea să efectueze astfel de teste). Prin urmare, testarea rezilienței operaționale digitale ar trebui să fie mai solicitantă pentru entitățile financiare semnificative (cum ar fi instituțiile de credit mari, bursele de valori, depozitarii centrali de titluri de valoare, contrapărțile centrale etc.). În același timp, testarea rezilienței operaționale digitale ar trebui să fie, de asemenea, mai relevantă pentru anumite subsectoare care joacă un rol sistemic esențial (de exemplu, plăți, servicii bancare, compensări și decontări) și mai puțin relevante pentru alte subsectoare (de exemplu, administratorii de active, agențiile de rating de credit etc.). Entitățile financiare transfrontaliere care își exercită libertatea de stabilire sau de prestare de servicii în Uniune ar trebui să respecte un singur set de cerințe de testare avansată (de exemplu, teste TLPT) în statul membru de origine, iar acest test ar trebui să includă infrastructurile TIC din toate jurisdicțiile în care grupul transfrontalier își desfășoară activitatea pe teritoriul Uniunii, permițând astfel grupurilor transfrontaliere să suporte costuri de testare într-o singură jurisdicție.

(45) Pentru a asigura o monitorizare solidă a riscurilor TIC generate de părți terțe, este necesar să se stabilească un set de norme bazate pe principii pentru a ghida monitorizarea efectuată de entitățile financiare în ceea ce privește riscurile care apar în contextul funcțiilor externalizate către furnizorii terți de servicii TIC și, în general, în contextul dependențelor de serviciile TIC furnizate de părți terțe.

(46) O entitate financiară ar trebui să rămână constant pe deplin responsabilă de respectarea obligațiilor prevăzute în prezentul regulament. Ar trebui să se organizeze o monitorizare proporțională a riscului care apare la nivelul furnizorului terț de servicii TIC, ținând seama în mod corespunzător de amploarea, complexitatea și importanța dependențelor legate de TIC, de caracterul critic sau de importanța serviciilor, proceselor sau funcțiilor care fac obiectul unor acorduri contractuale și, în ultimă instanță, pe baza unei evaluări atente a oricărui impact potențial asupra continuității și calității serviciilor financiare la nivel individual și de grup, după caz.

(47) Desfășurarea unei astfel de monitorizări ar trebui să urmeze o abordare strategică a riscurilor TIC generate de părți terțe, formalizată prin adoptarea de către organul de conducere al entității financiare a unei strategii dedicate, bazate pe o verificare continuă a tuturor acestor dependențe de servicii TIC furnizate de părți terțe. Pentru a spori gradul de sensibilizare a autorităților de supraveghere cu privire la dependențele de servicii TIC furnizate de părți terțe și cu scopul de a sprijini în continuare cadrul de supraveghere instituit prin prezentul regulament, autoritățile de supraveghere financiară ar trebui să primească în mod regulat informații esențiale din registre și să poată solicita extrase din acestea pe o bază ad-hoc.

(48) O analiză precontractuală amănunțită ar trebui să susțină și să preceadă încheierea oficială a acordurilor contractuale, în timp ce rezilierea contractelor ar trebui să fie determinată de cel puțin o serie de circumstanțe care indică deficiențe la nivelul furnizorului terț de servicii TIC.

(49) Pentru a aborda impactul sistemic al riscului de concentrare a serviciilor TIC furnizate de părți terțe, ar trebui promovată o soluție echilibrată bazată pe o abordare flexibilă și graduală întrucât plafoanele rigide sau limitările stricte pot stânjeni conduita în afaceri și libertatea contractuală. Entitățile financiare ar trebui să evalueze în detaliu acordurile contractuale pentru a identifica probabilitatea apariției unui astfel de risc, inclusiv prin intermediul unor analize aprofundate ale acordurilor de subcontractare a serviciilor externalizate, în special atunci când sunt încheiate cu furnizori terți de servicii TIC stabiliți într-o țară terță. În această etapă și în vederea găsirii unui echilibru între necesitatea imperativă de a menține libertatea contractuală și garantarea stabilității financiare, nu se consideră adecvat să se prevadă plafoane și limite stricte pentru expunerile la părți terțe din domeniul TIC. AES desemnată să efectueze supravegherea fiecărui furnizor terț esențial de servicii TIC („supraveghetorul principal”) ar trebui, în exercitarea atribuțiilor de supraveghere, să acorde o atenție deosebită înțelegerii pe deplin a amplorii interdependențelor și descoperirii situațiilor specifice în care un grad înalt de concentrare a furnizorilor terți esențiali de servicii TIC în Uniune ar putea exercita o presiune asupra stabilității și integrității sistemului financiar al Uniunii, trebuind să prevadă, în schimb, un dialog cu furnizorii terți esențiali de servicii TIC, în cazurile în care se identifică riscul respectiv[38].

(50) Pentru a putea evalua și monitoriza periodic capacitatea furnizorului terț de servicii TIC de a furniza în mod securizat entității financiare servicii fără efecte negative asupra rezilienței acesteia din urmă, ar trebui să existe o armonizare a elementelor contractuale cheie pe parcursul executării contractelor încheiate cu furnizorii terți de servicii TIC. Aceste elemente acoperă numai aspectele contractuale minime considerate esențiale pentru a permite monitorizarea deplină de către entitatea financiară din perspectiva asigurării rezilienței sale digitale care se bazează pe stabilitatea și securitatea serviciului TIC.

(51) Acordurile contractuale ar trebui să prevadă, în special, o specificare a descrierilor complete ale funcțiilor și serviciilor, a locațiilor în care astfel de funcții sunt furnizate și în care sunt prelucrate datele, precum și indicarea unor descrieri complete ale nivelului de servicii, însoțite de obiective cantitative și calitative privind performanța în limitele nivelurilor de servicii convenite, pentru a permite o monitorizare eficace de către entitatea financiară. În aceeași ordine de idei, dispozițiile privind accesibilitatea, disponibilitatea, integritatea, securitatea și protecția datelor cu caracter personal, precum și garanțiile privind accesul, redresarea și returnarea în caz de insolvență, de rezoluție sau de întrerupere a operațiunilor furnizorului terț de servicii TIC ar trebui, de asemenea, să fie considerate elemente esențiale pentru capacitatea unei entități financiare de a asigura monitorizarea riscului generat de părți terțe.

(52) Pentru a se asigura că entitățile financiare păstrează controlul deplin asupra tuturor evoluțiilor care pot afecta securitatea lor TIC, perioadele de preaviz și obligațiile de raportare ale furnizorului terț de servicii TIC ar trebui să fie stabilite în cazul unor evoluții cu un potențial impact semnificativ asupra capacității furnizorului terț de servicii TIC de a îndeplini în mod eficace funcții critice sau importante, inclusiv acordarea de asistență de către acesta din urmă în cazul unui incident legat de TIC, fără costuri suplimentare sau la un cost stabilit *ex-ante*.

---

[38] În plus, în cazul în care există un risc de abuz din partea unui furnizor terț de servicii TIC considerat dominant, entitățile financiare ar trebui să aibă, de asemenea, posibilitatea de a introduce o plângere oficială sau informală la Comisia Europeană sau la autoritățile naționale din domeniul dreptului concurenței.

(53) Drepturile de acces, de inspecție și de audit exercitate de entitatea financiară sau de o parte terță desemnată sunt instrumente esențiale în monitorizarea continuă de către entitățile financiare a performanței furnizorului terț de servicii TIC, alături de deplina cooperare a acestuia din urmă în timpul inspecțiilor. În aceeași ordine de idei, autoritatea competentă a entității financiare ar trebui să dispună de drepturile respective, pe baza unor notificări, pentru a inspecta și a audita furnizorul terț de servicii TIC, sub rezerva confidențialității.

(54) Acordurile contractuale ar trebui să prevadă drepturi clare de reziliere și perioade minime conexe de notificare, precum și strategii specifice de ieșire care să permită, în special, perioade de tranziție obligatorii în care furnizorii terți de servicii TIC să continue să furnizeze funcțiile relevante în vederea reducerii riscului de perturbări la nivelul entității financiare sau să permită acesteia să treacă efectiv la alți furnizori terți de servicii TIC sau, alternativ, să recurgă la utilizarea soluțiilor oferite la sediu, în concordanță cu complexitatea serviciului furnizat.

(55) În plus, utilizarea voluntară a clauzelor contractuale standard elaborate de Comisie pentru serviciile de cloud computing poate oferi mai mult confort entităților financiare și furnizorilor lor terți de servicii TIC, prin creșterea nivelului de securitate juridică cu privire la utilizarea serviciilor de cloud computing de către sectorul financiar, în conformitate deplină cu cerințele și așteptările prevăzute de regulamentul privind serviciile financiare. Această activitate se bazează pe măsurile prevăzute deja în Planul de acțiune privind FinTech din 2018, care a anunțat intenția Comisiei de a încuraja și a facilita elaborarea unor clauze contractuale standard pentru utilizarea externalizării serviciilor de cloud computing de către entitățile financiare, pe baza eforturilor părților interesate transsectoriale din domeniul serviciilor de cloud computing, pe care Comisia le-a facilitat cu ajutorul implicării sectorului financiar.

(56) Pentru a promova convergența și eficiența în ceea ce privește abordările în materie de supraveghere a riscurilor TIC generate de părți terțe la adresa sectorului financiar, pentru a consolida reziliența operațională digitală a entităților financiare care se bazează pe furnizorii terți esențiali de servicii TIC în scopul executării funcțiilor operaționale și, astfel, pentru a contribui la menținerea stabilității sistemului financiar al Uniunii, a integrității pieței unice a serviciilor financiare, furnizorii terți esențiali de servicii TIC ar trebui să facă obiectul unui cadru de supraveghere al Uniunii.

(57) Întrucât numai furnizorii terți esențiali de servicii necesită un tratament special, un mecanism de desemnare în scopul aplicării cadrului de supraveghere al Uniunii ar trebui instituit pentru a lua în considerare dimensiunea și natura dependenței sectorului financiar de astfel de furnizori terți de servicii TIC, ceea ce se traduce printr-un set de criterii cantitative și calitative care ar stabili parametrii criticității ca bază pentru includerea în activitățile de supraveghere. Furnizorii terți esențiali de servicii TIC care nu sunt desemnați în mod automat în temeiul aplicării criteriilor menționate mai sus ar trebui să aibă posibilitatea de a participa voluntar la cadrul de supraveghere, în timp ce furnizori terți de servicii TIC care fac deja obiectul cadrelor mecanismelor de supraveghere instituite la nivelul Eurosistemului cu scopul de a sprijini sarcinile menționate la articolul 127 alineatul (2) din Tratatul privind funcționarea Uniunii Europene ar trebui, prin urmare, să fie scutiți.

(58) Cerința privind constituirea în mod legal în Uniune a furnizorilor terți de servicii TIC care au fost desemnați ca fiind esențiali nu înseamnă o localizare a datelor, deoarece prezentul regulament nu implică nicio cerință suplimentară privind stocarea sau prelucrarea datelor, care să fie efectuată în Uniune.

(59) Acest cadru ar trebui să nu aducă atingere competenței statelor membre de a-și derula propriile misiuni de supraveghere cu privire la furnizorii terți de servicii TIC care nu sunt esențiali în temeiul prezentului regulament, dar care ar putea fi considerați importanți la nivel național.

(60) Pentru a valorifica actuala arhitectură instituțională pe mai multe niveluri în domeniul serviciilor financiare, Comitetul comun al AES ar trebui să asigure în continuare coordonarea transsectorială generală în ceea ce privește toate aspectele legate de riscurile TIC, în conformitate cu sarcinile sale privind securitatea cibernetică, sprijinit de un nou subcomitet (Forumul de supraveghere) care desfășoară activități pregătitoare atât pentru deciziile individuale adresate furnizorilor terți esențiali de servicii TIC, cât și pentru recomandările colective, în special cu privire la evaluarea comparativă a programelor de supraveghere a furnizorilor terți esențiali de servicii TIC, și care identifică cele mai bune practici pentru abordarea aspectelor legate de riscul de concentrare a serviciilor TIC.

(61) Pentru a asigura că furnizorii terți de servicii TIC care îndeplinesc un rol esențial pentru funcționarea sectorului financiar sunt supravegheați în mod proporțional la nivelul Uniunii, una dintre AES ar trebui desemnată drept supraveghetor principal pentru fiecare furnizor terț esențial de servicii TIC.

(62) Supraveghetorii principali trebuie să dispună de competențele necesare pentru a efectua investigații, inspecții la fața locului și inspecții la distanță la furnizorii terți esențiali de servicii TIC, pentru a accesa toate sediile și locațiile relevante și pentru a obține informații complete și actualizate care să le permită să dobândească o perspectivă reală asupra tipului, dimensiunii și impactului riscului TIC generat de partea terță pentru entitățile financiare și, în ultimă instanță, pentru sistemul financiar al Uniunii.

Încredințarea AES cu sarcina supravegherii principale este o condiție prealabilă pentru înțelegerea și abordarea dimensiunii sistemice a riscurilor TIC în domeniul finanțelor. Amprenta la nivelul Uniunii a furnizorilor terți esențiali de servicii TIC și eventualele probleme legate de riscul de concentrare a serviciilor TIC aferente acesteia necesită adoptarea unei abordări colective exercitate la nivelul Uniunii. Exercitarea unor drepturi multiple de audit și de acces de către numeroase autorități competente în mod separat, cu o coordonare redusă sau inexistentă, nu ar conduce la o imagine de ansamblu completă cu privire la riscurile TIC generate de părți terțe, creând în același timp o redundanță, o sarcină și o complexitate inutile la nivelul furnizorilor terți esențiali de servicii TIC care se confruntă cu numeroase astfel de solicitări.

(63) În plus, supraveghetorii principali ar trebui să poată prezenta recomandări cu privire la aspecte legate de riscurile TIC și la măsurile reparatorii adecvate, inclusiv să se opună anumitor acorduri contractuale care afectează în ultimă instanță stabilitatea entității financiare sau a sistemului financiar. Ca parte a funcției lor legate de supravegherea prudențială a entităților financiare, autoritățile naționale competente ar trebui să țină seama în mod corespunzător de respectarea acestor recomandări de fond prevăzute de supraveghetorii principali.

(64) Cadrul de supraveghere nu înlocuiește sau nu substituie în niciun fel și în nicio măsură gestionarea de către entitățile financiare a riscului pe care îl implică utilizarea furnizorilor terți de servicii TIC, inclusiv obligația de monitorizare continuă a acordurilor lor contractuale încheiate cu furnizori terți esențiali de servicii TIC, și nu afectează responsabilitatea deplină a entităților financiare de a respecta și a îndeplini toate cerințele prevăzute de prezentul regulament și de legislația relevantă privind

serviciile financiare. Pentru a evita duplicările și suprapunerile, autoritățile competente ar trebui să se abțină de la a lua în mod individual orice măsuri destinate monitorizării riscurilor implicate de furnizorul terț esențial de servicii TIC. Orice astfel de măsuri ar trebui să fie coordonate și convenite în prealabil, în contextul cadrului de supraveghere.

(65) Pentru a promova convergența la nivel internațional cu privire la cele mai bune practici care să fie utilizate în examinarea gestionării riscurilor digitale implicate de furnizorii terți de servicii TIC, AES ar trebui să fie încurajate să încheie acorduri de cooperare cu autoritățile de supraveghere și de reglementare competente relevante din țările terțe pentru a facilita elaborarea de bune practici în abordarea riscurilor TIC generate de părți terțe.

(66) Pentru a valorifica expertiza tehnică a experților autorităților competente în materie de gestionare a riscurilor operaționale și TIC, supraveghetorii principali ar trebui să apeleze la experiența națională în materie de supraveghere și să instituie echipe speciale de examinare pentru fiecare furnizor terț esențial de servicii TIC, reunind echipe multidisciplinare care să sprijine atât pregătirea, cât și executarea efectivă a activităților de supraveghere, inclusiv inspecții la fața locului ale furnizorilor terți esențiali de servicii TIC, precum și măsurile subsecvente necesare pentru aceștia.

(67) Autoritățile competente ar trebui să dețină toate competențele de supraveghere, de investigare și de sancționare necesare pentru a asigura aplicarea prezentului regulament. În principiu, sancțiunile administrative ar trebui să fie publicate. Întrucât entitățile financiare și furnizorii terți de servicii TIC se pot stabili în diferite state membre și pot face obiectul supravegherii unor autorități competente sectoriale diferite, ar trebui asigurată o cooperare strânsă între autoritățile competente relevante, inclusiv BCE în legătură cu sarcinile specifice atribuite acesteia prin Regulamentul (UE) nr. 1024/2013 al Consiliului[39], precum și consultarea cu AES prin schimbul reciproc de informații și acordarea de asistență reciprocă în contextul activităților de supraveghere.

(68) Pentru a cuantifica și a califica în continuare criteriile de desemnare pentru furnizorii terți esențiali de servicii TIC și pentru a armoniza taxele de supraveghere, competența de a adopta acte în conformitate cu articolul 290 din Tratatul privind funcționarea Uniunii Europene ar trebui delegată Comisiei în ceea ce privește: specificarea în continuare a impactului sistemic pe care neîndeplinirea obligațiilor de către un furnizor terț de servicii TIC ar putea să îl aibă asupra entităților financiare pe care le deservește, numărul de instituții de importanță sistemică globală (G-SII) sau de alte instituții de importanță sistemică (O-SII) care se bazează pe respectivul furnizor terț de servicii TIC, numărul de furnizori terți de servicii TIC activi pe o piață specifică, costurile migrației la un alt furnizor terț de servicii TIC, numărul de state membre în care furnizorul terț de servicii TIC relevant oferă serviciile și în care operează entitățile financiare care utilizează furnizorul terț de servicii TIC relevant, precum și valoarea taxelor de supraveghere și modalitatea de plată a acestora.

Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul

[39] Regulamentul (UE) nr. 1024/2013 al Consiliului din 15 octombrie 2013 de conferire a unor atribuții specifice Băncii Centrale Europene în ceea ce privește politicile legate de supravegherea prudențială a instituțiilor de credit (JO L 287, 29.10.2013, p. 63).

interinstituțional din 13 aprilie 2016 privind o mai bună legiferare[40]. În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții statelor membre, iar experții acestora au acces în mod sistematic la reuniunile grupurilor de experți ale Comisiei, însărcinate cu pregătirea actelor delegate.

(69) Întrucât prezentul regulament, împreună cu Directiva (UE) 20xx/xx a Parlamentului European și a Consiliului[41], implică o consolidare a dispozițiilor privind gestionarea riscurilor TIC din mai multe regulamente și directive din acquis-ul Uniunii privind serviciile financiare, inclusiv Regulamentele (CE) nr. 1060/2009, (UE) nr. 648/2012 (UE) nr. 600/2014 și (UE) nr. 909/2014, pentru a asigura coerența deplină, regulamentele respective ar trebui să fie modificate pentru a clarifica faptul că dispozițiile relevante privind riscurile TIC sunt prevăzute în prezentul regulament.

Standardele tehnice ar trebui să asigure armonizarea consecventă a cerințelor prevăzute în prezentul regulament. În calitate de organisme cu expertiză foarte specializată, AES ar trebui să fie împuternicite să elaboreze proiecte de standarde tehnice de reglementare care nu implică opțiuni de politică, pe care să le înainteze Comisiei. Standardele tehnice de reglementare ar trebui să fie elaborate în domeniul gestionării riscurilor TIC, al raportării și al testării cu privire la acestea, precum și al cerințelor-cheie legate de ele, pentru o monitorizare solidă a riscurilor TIC generate de părți terțe.

(70) Este deosebit de important ca, în cadrul activității sale pregătitoare, Comisia să desfășoare consultări corespunzătoare, inclusiv la nivel de experți. Comisia și AES ar trebui să se asigure că standardele și cerințele respective pot fi aplicate de toate instituțiile financiare într-o manieră proporțională cu natura, amploarea și complexitatea instituțiilor respective și a activităților acestora.

(71) Pentru a facilita comparabilitatea rapoartelor privind incidentele majore legate de TIC și pentru a asigura transparența cu privire la acordurile contractuale pentru utilizarea serviciilor TIC oferite de furnizorii terți de servicii TIC, AES ar trebui să fie mandatate să elaboreze proiecte de standarde tehnice de punere în aplicare, care să stabilească modele, formulare și proceduri standardizate pentru ca entitățile financiare să raporteze incidentele majore legate de TIC, precum și modele standardizate pentru înregistrarea informațiilor. În elaborarea acestor standarde, AES ar trebui să țină seama de dimensiunea și de complexitatea entităților financiare, precum și de natura și nivelul de risc aferente activităților lor. Comisia ar trebui să fie împuternicită să adopte standardele tehnice de punere în aplicare respective prin intermediul unor acte de punere în aplicare, în temeiul articolului 291 din TFUE și al articolului 15 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și, respectiv, (UE) nr. 1095/2010. Întrucât au fost deja specificate cerințe suplimentare prin intermediul actelor delegate și al actelor de punere în aplicare, pe baza standardelor tehnice de reglementare și de punere în aplicare din Regulamentele (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014 și, respectiv, (UE) nr. 909/2014, este adecvat ca AES să fie mandatate, fie individual, fie în comun, prin intermediul Comitetului comun, să prezinte Comisiei standarde tehnice de reglementare și de punere în aplicare pentru adoptarea actelor delegate și de punere în aplicare care preiau și actualizează normele existente privind gestionarea riscurilor TIC.

---

40 JO L 123, 12.5.2016, p. 1.

41 [*a se introduce referința completă*].

(72) Acest exercițiu va presupune modificarea ulterioară a actelor delegate și de punere în aplicare existente, adoptate în diferite domenii ale legislației privind serviciile financiare. Domeniul de aplicare al articolelor privind riscul operațional, în temeiul cărora împuternicirile acordate în cadrul acestor acte au mandatat adoptarea de acte delegate și de punere în aplicare, ar trebui să fie modificat în vederea preluării în prezentul regulament a tuturor dispozițiilor referitoare la reziliența operațională digitală care fac parte astăzi din regulamentele respective.

(73) Deoarece obiectivul prezentului regulament, și anume atingerea unui nivel ridicat de reziliență operațională digitală aplicabil tuturor entităților financiare, nu poate fi realizat în mod suficient de statele membre deoarece implică armonizarea unui număr semnificativ de norme diferite care există, în prezent, fie în unele acte ale Uniunii, fie în sistemele juridice ale diverselor state membre, dar, având în vedere amploarea și efectele sale, poate fi realizat mai bine la nivelul Uniunii, Uniunea poate adopta măsuri în conformitate cu principiul subsidiarității, astfel cum este definit la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este enunțat la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru atingerea obiectivului respectiv.

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

DISPOZIȚII GENERALE

Articolul 1

Obiectul

1. Prezentul regulament stabilește următoarele cerințe uniforme privind securitatea rețelelor și a sistemelor informatice care susțin procesele operaționale ale entităților financiare, necesare pentru a atinge un nivel comun ridicat de reziliență operațională digitală, după cum urmează:

   (a) cerințe aplicabile entităților financiare în legătură cu:

   – gestionarea riscurilor legate de tehnologia informației și comunicațiilor (TIC);

   – raportarea incidentelor majore legate de TIC către autoritățile competente;

   – testarea rezilienței operaționale digitale;

   – schimbul de informații și de date operative cu privire la amenințările și vulnerabilitățile cibernetice;

   – măsuri pentru o bună gestionare de către entitățile financiare a riscurilor TIC generate de părți terțe;

   (b) cerințe în legătură cu acordurile contractuale încheiate între furnizorii terți de servicii TIC și entitățile financiare;

   (c) cadrul de supraveghere pentru furnizorii terți esențiali de servicii TIC, atunci când furnizează servicii entităților financiare;

   (d) normele privind cooperarea între autoritățile competente și normele privind supravegherea și asigurarea respectării de către autoritățile competente în legătură cu toate aspectele vizate de prezentul regulament.

2. În ceea ce privește entitățile financiare identificate drept operatori de servicii esențiale în temeiul normelor naționale care transpun articolul 5 din Directiva (UE) 2016/1148, prezentul regulament este considerat drept act juridic al Uniunii specific unui sector în sensul articolului 1 alineatul (7) din directiva respectivă.

Articolul 2

Domeniul de aplicare personal

1. Prezentul regulament se aplică următoarelor entități:

(a) instituții de credit;

(b) instituții de plată;

(c) instituții emitente de monedă electronică;

(d) firme de investiții;

(e) furnizori de servicii de criptoactive, emitenți de criptoactive, emitenți de tokenuri raportate la active și emitenți de tokenuri semnificative raportate la active;

(f) depozitari centrali de titluri de valoare;

(g) contrapărți centrale;

(h) locuri de tranzacționare;

(i) registre centrale de tranzacții;

(j) administratori de fonduri de investiții alternative;

(k) societăți de administrare;

(l) furnizori de servicii de raportare a datelor;

(m) întreprinderi de asigurare și de reasigurare;

(n) intermediari de asigurări, intermediari de reasigurări și intermediari de asigurări auxiliare;

(o) instituții pentru furnizarea de pensii ocupaționale;

(p) agenții de rating de credit;

(q) auditori statutari și societăți de audit;

(r) administratori ai indicilor de referință critici;

(s) furnizori de servicii de finanțare participativă;

(t) registre centrale de securitizări;

(u) furnizori terți de servicii TIC.

2. În sensul prezentului regulament, entitățile menționate la literele (a)-(t) sunt denumite colectiv „entități financiare”.

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

(1) „reziliență operațională digitală” înseamnă capacitatea unei entități financiare de a construi, a asigura și a revizui integritatea sa operațională din perspectivă tehnologică, prin asigurarea, în mod direct sau indirect, utilizând servicii ale furnizorilor terți de servicii TIC, a întregii game a capacităților legate de TIC necesare pentru a aborda securitatea rețelelor și a sistemelor informatice pe care le utilizează o entitate financiară și care sprijină furnizarea continuă de servicii financiare și calitatea acestora;

(2) „rețea și sistem informatic” înseamnă rețeaua și sistemul informatic astfel cum sunt definite la articolul 4 punctul 1 din Directiva (UE) 2016/1148;

(3) „securitatea rețelelor și a sistemelor informatice” înseamnă securitatea rețelelor și a sistemelor informatice astfel cum este definită la articolul 4 punctul 2 din Directiva (UE) 2016/1148;

(4) „risc TIC” înseamnă orice circumstanță care poate fi identificată în mod rezonabil în legătură cu utilizarea rețelelor și a sistemelor informatice – inclusiv o disfuncționalitate, o depășire a capacității, o defecțiune, o perturbare, o deteriorare, o utilizare necorespunzătoare, o pierdere sau un alt tip de eveniment răuvoitor sau fără rea intenție, care, dacă s-a materializat, poate compromite securitatea rețelelor și a sistemelor informatice, a oricărui instrument sau proces dependent de tehnologie, a operării și a derulării unui proces sau a prestării de servicii, compromițând, astfel, integritatea sau disponibilitatea datelor, a software-ului sau a oricărei alte componente a serviciilor și infrastructurilor TIC sau cauzând o încălcare a confidențialității, o deteriorare a infrastructurii fizice TIC sau alte efecte negative;

(5) „activ informațional” înseamnă o colecție de informații, materială sau imaterială, care merită protejată;

(6) „incident legat de TIC” înseamnă un eveniment identificat neprevăzut în rețele și sistemele de informații, indiferent dacă rezultă dintr-o activitate răuvoitoare sau nu, care compromite securitatea rețelelor și a sistemelor informatice, a informațiilor pe care aceste sisteme le prelucrează, le stochează sau le transmit sau care are efecte negative asupra disponibilității, a confidențialității, a continuității sau a autenticității serviciilor financiare furnizate de entitatea financiară;

(7) „incident major legat de TIC” înseamnă un incident legat de TIC care poate avea un impact negativ puternic asupra rețelelor și a sistemelor informatice care sprijină funcțiile critice ale entității financiare;

(8) „amenințare cibernetică” înseamnă „amenințare cibernetică” astfel cum este definită la articolul 2 punctul 8 din Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[42];

(9) „atac cibernetic” înseamnă un incident legat de TIC rău-intenționat, care are loc prin încercarea de a distruge, a expune, a modifica, a dezactiva, a fura sau a obține acces neautorizat la un activ ori a utiliza în mod neautorizat un activ, comis de orice entitate răuvoitoare;

[42] 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).

(10) „date operative privind amenințările” înseamnă informații care au fost agregate, transformate, analizate, interpretate sau îmbogățite pentru a oferi contextul necesar procesului decizional și care asigură o înțelegere adecvată și suficientă pentru a atenua impactul unui incident legat de TIC sau al unei amenințări cibernetice, inclusiv detaliile tehnice ale unui atac cibernetic, persoanele responsabile de atac și modul de operare și motivațiile acestora;

(11) „apărare în profunzime” înseamnă o strategie în domeniul TIC care integrează persoane, procese și tehnologii pentru a crea o gamă variată de bariere pe mai multe straturi și dimensiuni ale entității;

(12) „vulnerabilitate” înseamnă un punct slab, o susceptibilitate sau un defect al unui activ, sistem, proces sau control care poate fi exploatat de o amenințare;

(13) „test de penetrare bazat pe amenințări” înseamnă un cadru care imită tacticile, tehnicile și procedurile utilizate de entitățile răuvoitoare din viața reală, percepute ca reprezentând o amenințare cibernetică autentică, și care asigură un test controlat, personalizat, bazat pe informații (de tip „echipa roșie”) al sistemelor critice de producție în timp real ale entității;

(14) „risc TIC generat de părți terțe” înseamnă un risc TIC care poate apărea pentru o entitate financiară în legătură cu utilizarea, de către aceasta, a serviciilor TIC oferite de furnizori terți de servicii TIC sau de subcontractanți ai acestora din urmă;

(15) „furnizor terț de servicii TIC” înseamnă o întreprindere care furnizează servicii digitale și de date, inclusiv furnizori de servicii de cloud computing, software, servicii de analiză de date, centre de date, cu excepția furnizorilor de componente hardware și a entităților autorizate în temeiul dreptului Uniunii, care furnizează servicii de comunicații electronice, astfel cum sunt definite la articolul 2 punctul 4 din Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului[43];

(16) „servicii TIC” înseamnă servicii digitale și de date furnizate prin intermediul sistemelor TIC către unul sau mai mulți utilizatori interni sau externi, inclusiv furnizarea de date, introducerea de date, stocarea de date, servicii de prelucrare și de raportare de date, monitorizarea datelor, precum și servicii de sprijinire a întreprinderilor și a deciziilor bazate pe date;

(17) „funcție critică sau importantă” înseamnă o funcție a cărei execuție întreruptă, deficientă sau eșuată ar afecta în mod semnificativ respectarea în continuare, de către o entitate financiară, a condițiilor și obligațiilor aferente autorizației sale sau a altor obligații care îi revin în temeiul legislației aplicabile în domeniul serviciilor financiare, ori performanța sa financiară sau soliditatea sau continuitatea serviciilor și activităților sale;

(18) „furnizor terț esențial de servicii TIC” înseamnă un furnizor terț de servicii TIC desemnat în conformitate cu articolul 29 și care face obiectul cadrului de supraveghere menționat la articolele 30-37;

(19) „furnizor terț de servicii TIC stabilit într-o țară terță” înseamnă un furnizor terț de servicii TIC care este o persoană juridică stabilită într-o țară terță, care nu a înființat o societate/nu este prezentă în Uniune și care a încheiat un acord contractual cu o entitate financiară pentru furnizarea de servicii TIC;

[43] Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice (reformare) (JO L 321, 17.12.2018, p. 36).

(20) „subcontractant TIC stabilit într-o țară terță” înseamnă un subcontractant TIC care este o persoană juridică stabilită într-o țară terță, care nu a înființat o societate/nu este prezentă în Uniune și care a încheiat un acord contractual fie cu un furnizor terț de servicii TIC, fie cu un furnizor terț de servicii TIC stabilit într-o țară terță;

(21) „risc de concentrare a serviciilor TIC” înseamnă o expunere la furnizori terți esențiali de servicii TIC individuali sau multipli, care creează un grad de dependență față de acești furnizori, astfel încât indisponibilitatea, intrarea în dificultate sau alt tip de deficiență a acestora din urmă poate pune în pericol capacitatea unei entități financiare și, în cele din urmă, a sistemului financiar al Uniunii în ansamblul său, de a îndeplini funcții critice sau de a suporta alte tipuri de efecte adverse, inclusiv pierderi mari;

(22) „organ de conducere” înseamnă un organ de conducere astfel cum este definit la articolul 4 alineatul (1) punctul 36 din Directiva 2014/65/UE, la articolul 3 alineatul (1) punctul 7 din Directiva 2013/36/UE, la articolul 2 alineatul (1) litera (s) din Directiva 2009/65/CE, la articolul 2 alineatul (1) punctul 45 din Regulamentul (UE) nr. 909/2014, la articolul 3 alineatul (1) punctul 20 din Regulamentul (UE) 2016/1011 al Parlamentului European și al Consiliului[44], la articolul 3 alineatul (1) litera (u) din Regulamentul (UE) 20xx/xx al Parlamentului European și al Consiliului[45] [MICA] sau persoanele echivalente care conduc efectiv entitatea sau dețin funcții-cheie în conformitate cu legislația Uniunii sau cu legislația națională relevantă;

(23) „instituție de credit” se referă la o instituție de credit astfel cum este definită la articolul 4 alineatul (1) punctul 1 din Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului[46];

(24) „firmă de investiții” înseamnă o firmă de investiții astfel cum este definită la articolul 4 alineatul (1) punctul 1 din Directiva 2014/65/UE;

(25) „instituție de plată” înseamnă o instituție de plată astfel cum este definită la articolul 1 alineatul (1) litera (d) din Directiva (UE) 2015/2366;

(26) „instituție emitentă de monedă electronică” înseamnă o instituție emitentă de monedă electronică astfel cum este definită la articolul 2 punctul 1 din Directiva 2009/110/CE a Parlamentului European și a Consiliului[47];

(27) „contraparte centrală” înseamnă o contraparte centrală astfel cum este definită la articolul 2 punctul 1 din Regulamentul (UE) nr. 648/2012;

(28) „registru central de tranzacții” înseamnă un registru central de tranzacții astfel cum este definit la articolul 2 punctul 2 din Regulamentul (UE) nr. 648/2012;

---

44 Regulamentul (UE) 2016/1011 al Parlamentului European și al Consiliului din 8 iunie 2016 privind indicii utilizați ca indici de referință în cadrul instrumentelor financiare și al contractelor financiare sau pentru a măsura performanțele fondurilor de investiții și de modificare a Directivelor 2008/48/CE și 2014/17/UE și a Regulamentului (UE) nr. 596/2014 (JO L 171, 29.6.2016, p. 1).

45 [*a se introduce titlul complet și referința din JO*].

46 Regulamentul nr. 575/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și societățile de investiții și de modificare a Regulamentului (UE) nr. 648/2012 (JO L 176, 27.6.2013, p. 1).

47 Directiva 2009/110/CE a Parlamentului European și a Consiliului din 16 septembrie 2009 privind accesul la activitate, desfășurarea și supravegherea prudențială a activității instituțiilor emitente de monedă electronică, de modificare a Directivelor 2005/60/CE și 2006/48/CE și de abrogare a Directivei 2000/46/CE (JO L 267, 10.10.2009, p. 7).

(29) „depozitar central de titluri de valoare” înseamnă un depozitar central de titluri de valoare astfel cum este definit la articolul 2 alineatul (1) punctul 1 din Regulamentul (UE) nr. 909/2014;

(30) „loc de tranzacționare” înseamnă un loc de tranzacționare astfel cum este definit la articolul 4 alineatul (1) punctul 24 din Directiva 2014/65/UE;

(31) „administrator de fonduri de investiții alternative” înseamnă un administrator de fonduri de investiții alternative astfel cum este definit la articolul 4 alineatul (1) litera (b) din Directiva 2011/61/UE;

(32) „societate de administrare” înseamnă o societate de administrare astfel cum este definită la articolul 2 alineatul (1) litera (b) din Directiva 2009/65/CE;

(33) „furnizor de servicii de raportare a datelor” înseamnă un furnizor de servicii de raportare a datelor astfel cum este definit la articolul (4) alineatul (1) punctul (63) din Directiva 2014/65/UE;

(34) „întreprindere de asigurare” înseamnă o întreprindere de asigurare astfel cum este definită la articolul 13 punctul 1 din Directiva 2009/138/CE;

(35) „întreprindere de reasigurare” înseamnă o întreprindere de reasigurare astfel cum este definită la articolul 13 punctul 4 din Directiva 2009/138/CE;

(36) „intermediar de asigurări” înseamnă un intermediar de asigurări astfel cum este definit la articolul 2 punctul 3 din Directiva (UE) 2016/97;

(37) „intermediar de asigurări auxiliare” înseamnă un intermediar de asigurări auxiliare astfel cum este definit la articolul 2 punctul 4 din Directiva (UE) 2016/97;

(38) „intermediar de reasigurări” înseamnă un intermediar de reasigurări astfel cum este definit la articolul 2 punctul 5 din Directiva (UE) 2016/97;

(39) „instituție pentru furnizarea de pensii ocupaționale” înseamnă instituția pentru furnizarea de pensii ocupaționale astfel cum este definită la articolul 6 punctul 1 din Directiva 2016/2341;

(40) „agenție de rating de credit” înseamnă o agenție de rating de credit astfel cum este definită la articolul 3 alineatul (1) litera (b) din Regulamentul (CE) nr. 1060/2009;

(41) „auditor statutar” înseamnă un auditor legal astfel cum este definit la articolul 2 punctul 2 din Directiva 2006/43/CE;

(42) „firmă de audit” înseamnă o firmă de audit astfel cum este definită la articolul 2 punctul 3 din Directiva 2006/43/CE;

(43) „furnizor de servicii de criptoactive” înseamnă un furnizor de servicii de criptoactive astfel cum este definit la articolul 3 alineatul (1) litera (n) din Regulamentul (UE) 202x/xx [*OP: a se introduce referința la Regulamentul MiCA*];

(44) „emitent de criptoactive” înseamnă un emitent de criptoactive astfel cum este definit la articolul 3 alineatul (1) litera (h) din [*JO: a se introduce referința la Regulamentul MiCA*];

(45) „emitent de tokenuri raportate la active” înseamnă un emitent de tokenuri raportate la active astfel cum este definit la articolul 3 alineatul (1) punctul (i) din [*JO: a se introduce referința la Regulamentul MiCA*];

(46) „emitent de tokenuri semnificative raportate la active” înseamnă un emitent de tokenuri semnificative raportate la active astfel cum este definit la articolul 3 alineatul (1) litera (j) din [*JO: a se introduce referința la Regulamentul MiCA*];

(47) „administrator al indicilor de referință critici” înseamnă un administrator al indicilor de referință critici astfel cum este definit la articolul x punctul x din Regulamentul xx/202x [*JO: a se introduce referința la Regulamentul indicilor de referință*];

(48) „furnizor de servicii de finanțare participativă” înseamnă un furnizor de servicii de finanțare participativă astfel cum este definit la articolul x punctul x din Regulamentul (UE) 202x/xx [*OP: a se introduce referința la Regulamentul privind finanțarea participativă*];

(49) „registru central de securitizări” înseamnă un registru central de securitizări astfel cum este definit la articolul 2 punctul 23 din Regulamentul (UE) 2017/2402;

(50) „microîntreprindere” înseamnă o entitate financiară astfel cum este definită la articolul 2 alineatul (3) din anexa la Recomandarea 2003/361/CE.

CAPITOLUL II

GESTIONAREA RISCURILOR TIC

SECȚIUNEA I

Articolul 4

Guvernanță și organizare

1. Entitățile financiare dispun de cadre interne de guvernanță și control care asigură o gestionare eficace și prudentă a tuturor riscurilor TIC.

2. Organul de conducere al entității financiare definește, aprobă, supraveghează și este responsabil de punerea în aplicare a tuturor dispozițiilor legate de cadrul de gestionare a riscurilor TIC menționat la articolul 5 alineatul (1):

   În sensul primului paragraf, organul de conducere:

   (a) poartă responsabilitatea finală pentru gestionarea riscurilor TIC ale entității financiare;

   (b) stabilește roluri și responsabilități clare pentru toate funcțiile legate de TIC;

   (c) determină nivelul adecvat de toleranță la risc pentru riscurile TIC în cazul entității financiare, astfel cum se menționează la articolul 5 alineatul (9) litera (b);

   (d) aprobă, supraveghează și verifică periodic punerea în aplicare a politicii de continuitate a activității bazate pe TIC și a planului de recuperare a capabilităților TIC în caz de dezastru ale entității financiare, menționate la articolul 10 alineatele (1) și (3);

   (e) aprobă și verifică periodic planurile de audit al TIC, auditurile TIC și modificările semnificative aduse acestora;

   (f) alocă și verifică periodic bugetul adecvat pentru a răspunde nevoilor de reziliență operațională digitală ale entității financiare în ceea ce privește toate

tipurile de resurse, inclusiv formarea cu privire la riscurile și competențele TIC pentru toți membrii personalului relevant;

(g) aprobă și verifică periodic politica entității financiare cu privire la modalitățile de utilizare a serviciilor TIC oferite de furnizori terți de servicii TIC;

(h) este informat în mod corespunzător cu privire la acordurile încheiate cu furnizorii terți de servicii TIC pentru utilizarea serviciilor TIC, la orice modificări semnificative planificate relevante privind furnizorii terți de servicii TIC și la impactul potențial al unor astfel de modificări asupra funcțiilor critice sau importante care fac obiectul acestor acorduri, inclusiv primirea unui rezumat al analizei de risc pentru a evalua impactul acestor modificări;

(i) este informat în mod corespunzător cu privire la incidentele legate de TIC și impactul lor, precum și la răspunsul la acestea, recuperarea și măsurile corective.

3. Entitățile financiare, altele decât microîntreprinderile, stabilesc un rol de monitorizare a acordurilor încheiate cu furnizorii terți de servicii TIC cu privire la utilizarea serviciilor TIC sau desemnează un membru al conducerii de nivel superior drept responsabil de supravegherea expunerii la risc aferente și a documentației relevante.

4. Membrii organului de conducere urmează periodic cursuri de formare specifice pentru a dobândi cunoștințe și competențe suficiente pentru a înțelege și a evalua riscurile TIC și impactul acestora asupra operațiunilor entității financiare, precum și pentru a menține actualizate cunoștințele și competențele respective.

SECȚIUNEA II

Articolul 5

Cadrul de gestionare a riscurilor TIC

1. Entitățile financiare dispun de un cadru solid, cuprinzător și bine documentat de gestionare a riscurilor TIC, care le permite să abordeze riscurile TIC în mod rapid, eficient și cuprinzător și să asigure un nivel ridicat de reziliență operațională digitală, care corespunde nevoilor, dimensiunii și complexității activității lor.

2. Cadrul de gestionare a riscurilor TIC menționat la alineatul (1) include strategii, politici, proceduri, protocoale și instrumente TIC, care sunt necesare pentru a proteja în mod corespunzător și eficace toate componentele și infrastructurile fizice relevante, inclusiv componentele hardware ale calculatoarelor, serverele, precum și toate sediile relevante, centrele de date și zonele desemnate sensibile, pentru a asigura că toate elementele fizice respective sunt protejate în mod adecvat împotriva riscurilor, inclusiv împotriva pagubelor și a accesului sau utilizării neautorizate.

3. Entitățile financiare reduc la minimum impactul riscurilor TIC prin utilizarea strategiilor, politicilor, procedurilor, protocoalelor și instrumentelor adecvate, astfel cum se stabilește în cadrul de gestionare a riscurilor TIC. Acestea furnizează informații complete și actualizate cu privire la riscurile TIC, conform cerințelor autorităților competente.

4. Ca parte a cadrului de gestionare a riscurilor TIC menționat la alineatul (1), entitățile financiare, altele decât microîntreprinderile, pun în aplicare un sistem de gestionare a securității informațiilor bazat pe standarde internaționale recunoscute și în

conformitate cu orientările în materie de supraveghere și revizuiesc periodic acest sistem.

5. Entitățile financiare, altele decât microîntreprinderile, asigură o separare adecvată a funcțiilor de gestionare a riscurilor TIC, a funcțiilor de control și a funcțiilor de audit intern, în conformitate cu cele trei linii ale modelului de apărare sau cu un model intern de gestionare și control al riscurilor.

6. Cadrul de gestionare a riscurilor TIC menționat la alineatul (1) se documentează și se revizuiește cel puțin o dată pe an, precum și în cazul unor incidente majore legate de TIC și în urma instrucțiunilor sau concluziilor în materie de supraveghere care decurg din testele relevante privind reziliența operațională digitală sau din procesele de audit relevante. Acesta este îmbunătățit în permanență, pe baza învățămintelor desprinse în urma punerii în aplicare și a monitorizării.

7. Cadrul de gestionare a riscurilor TIC menționat la alineatul (1) este auditat periodic de către auditorii TIC care posedă suficiente cunoștințe, competențe și expertiză în ceea ce privește riscurile TIC. Frecvența și obiectivul auditurilor TIC sunt proporționale cu riscurile TIC ale entității financiare.

8. Se instituie un proces formal de monitorizare, inclusiv norme pentru verificarea și remedierea în timp util a elementelor critice constatate în cadrul auditurilor TIC, luând în considerare concluziile evaluării de audit și ținând totodată seama în mod corespunzător de natura, amploarea și complexitatea serviciilor și activităților entităților financiare.

9. Cadrul de gestionare a riscurilor TIC menționat la alineatul (1) include o strategie privind reziliența digitală care stabilește modul de punere în aplicare a cadrului. În acest scop, strategia include metodele de abordare a riscurilor TIC și de realizare a obiectivelor TIC specifice, prin:

   (a) explicarea modului în care cadrul de gestionare a riscurilor TIC sprijină strategia de afaceri și obiectivele entității financiare;

   (b) stabilirea nivelului de toleranță la risc pentru riscurile TIC, în conformitate cu apetitul pentru risc al entității financiare, și analizarea toleranței la impactul perturbărilor TIC;

   (c) stabilirea unor obiective clare privind securitatea informațiilor;

   (d) explicarea arhitecturii de referință TIC și a oricăror modificări necesare pentru atingerea obiectivelor specifice de activitate;

   (e) prezentarea diferitelor mecanisme instituite pentru a detecta, a proteja și a preveni impactul incidentelor legate de TIC;

   (f) evidențierea numărului de incidente majore legate de TIC raportate și a eficacității măsurilor preventive;

   (g) definirea unei strategii TIC holistice pentru furnizori multipli la nivel de entitate, care să arate principalele dependențe față de furnizorii terți de servicii TIC și să explice raționamentul care stă la baza mixului de achiziții de la furnizori terți de servicii;

   (h) punerea în aplicare a testării privind reziliența operațională digitală;

   (i) descrierea unei strategii de comunicare în cazul unor incidente legate de TIC.

10. În urma aprobării de către autoritățile competente, entitățile financiare pot delega sarcinile de verificare a conformității cu cerințele de gestionare a riscurilor TIC către entități intragrup sau externe.

Articolul 6

Sisteme, protocoale și instrumente TIC

1. Entitățile financiare utilizează și mențin sisteme, protocoale și instrumente TIC actualizate, care îndeplinesc următoarele condiții:

   (a) sistemele și instrumentele sunt adecvate naturii, varietății, complexității și magnitudinii operațiunilor care sprijină desfășurarea activităților lor;

   (b) sunt fiabile;

   (c) dispun de o capacitate suficientă pentru a prelucra cu precizie datele necesare pentru desfășurarea activităților și furnizarea serviciilor în timp util, precum și pentru a face față volumelor ridicate de ordine, mesaje sau tranzacții, după caz, inclusiv în cazul introducerii unor noi tehnologii;

   (d) sunt reziliente din punct de vedere tehnologic pentru a face față în mod adecvat nevoilor suplimentare de prelucrare a informațiilor, astfel cum se dovedește necesar în condiții de criză a pieței sau în alte situații nefavorabile.

2. În cazul în care utilizează standarde tehnice recunoscute la nivel internațional și practicile principale din sector privind securitatea informațiilor și controalele interne privind TIC, entitățile financiare utilizează standardele și practicile respective în concordanță cu orice recomandare în materie de supraveghere relevantă privind integrarea lor.

Articolul 7

Identificare

1. Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 5 alineatul (1), entitățile financiare identifică, clasifică și documentează în mod corespunzător toate funcțiile de activitate legate de TIC, activele informaționale care sprijină aceste funcții, precum și configurațiile sistemului TIC și interconexiunile cu sistemele TIC interne și externe. Entitățile financiare revizuiesc, după caz, dar cel puțin anual, caracterul adecvat al clasificării activelor informaționale și a oricăror documente relevante.

2. Entitățile financiare identifică în mod constant toate sursele de riscuri TIC, în special expunerea la riscuri față de alte entități financiare și din partea altor entități financiare, și evaluează amenințările cibernetice și vulnerabilitățile TIC relevante pentru funcțiile legate de TIC și activele lor informaționale. Entitățile financiare revizuiesc în mod regulat și cel puțin o dată pe an scenariile de risc care au un impact asupra lor.

3. Entitățile financiare, altele decât microîntreprinderile, efectuează o evaluare a riscurilor cu ocazia fiecărei modificări majore aduse infrastructurii rețelei și a sistemului informatic, proceselor sau procedurilor care le afectează funcțiile, procesele de sprijin sau activele informaționale.

4. Entitățile financiare identifică toate conturile sistemelor TIC, inclusiv cele din locații îndepărtate, resursele de rețea și echipamentele hardware și cartografiază echipamentele fizice considerate esențiale. Acestea cartografiază configurația activelor TIC și legăturile și interdependențele dintre diferitele active TIC.

5. Entitățile financiare identifică și documentează toate procesele care depind de furnizorii terți de servicii TIC și identifică interconexiunile cu furnizorii terți de servicii TIC.

6. În sensul alineatelor (1), (4) și (5), entitățile financiare mențin și actualizează periodic inventarele relevante.

7. Entitățile financiare, altele decât microîntreprinderile, efectuează periodic și cel puțin o dată pe an o evaluare specifică a riscurilor TIC vizând toate sistemele TIC deja existente, în special înainte și după conectarea tehnologiilor, aplicațiilor sau sistemelor vechi cu cele noi.

Articolul 8

Protecție și prevenire

1. În scopul protejării adecvate a sistemelor TIC și în vederea organizării măsurilor de răspuns, entitățile financiare monitorizează și controlează în mod continuu funcționarea sistemelor și a instrumentelor TIC și reduc la minimum impactul unor astfel de riscuri prin utilizarea instrumentelor, politicilor și procedurilor de securitate TIC adecvate.

2. Entitățile financiare concep, achiziționează și pun în aplicare strategii, politici, proceduri, protocoale și instrumente în domeniul securității TIC care vizează, în special, asigurarea rezilienței, a continuității și a disponibilității sistemelor TIC, precum și menținerea unor standarde înalte de securitate, confidențialitate și integritate a datelor, indiferent dacă sunt în repaus, în uz sau în tranzit.

3. Pentru a îndeplini obiectivele menționate la alineatul (2), entitățile financiare utilizează tehnologii și procese TIC de ultimă generație, care:

   (a) garantează securitatea mijloacelor de transfer al informațiilor;

   (b) reduc la minimum riscul de corupere sau de pierdere a datelor, de acces neautorizat și de defecțiuni tehnice care pot împiedica derularea activităților;

   (c) împiedică scurgerile de informații;

   (d) asigură protecția datelor împotriva gestionării deficitare sau a riscurilor legate de prelucrare, inclusiv a evidenței neadecvate.

4. Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 5 alineatul (1), entitățile financiare:

   (a) elaborează și documentează o politică de securitate a informațiilor care definește norme de protecție a confidențialității, integrității și disponibilității resurselor TIC, datelor și activelor informaționale proprii și a celor ale clienților;

   (b) aplicând o abordare bazată pe riscuri, stabilesc o gestionare solidă a rețelei și a infrastructurii, utilizând tehnici, metode și protocoale adecvate, inclusiv punerea în aplicare a unor mecanisme automatizate pentru a izola activele informaționale afectate în cazul unor atacuri cibernetice;

(c) pun în aplicare politici care limitează accesul fizic și virtual la resursele și datele din sistemul TIC la ceea ce este necesar numai pentru funcții și activități legitime și aprobate și stabilesc în acest scop un set de politici, proceduri și controale care să abordeze privilegiile de acces și o bună gestionare a acestora;

(d) pun în aplicare politici și protocoale pentru mecanisme solide de autentificare, bazate pe standarde relevante și sisteme de control specifice pentru a preveni accesul la chei criptografice prin care datele sunt criptate în funcție de rezultatele proceselor aprobate de clasificare a datelor și de evaluare a riscurilor;

(e) pun în aplicare politici, proceduri și controale pentru gestionarea modificărilor la nivelul TIC, inclusiv schimbări ale componentelor software, hardware, firmware, modificări ale sistemelor sau modificări de securitate, care sunt fondate pe o abordare bazată pe evaluarea riscurilor și fac parte integrantă din procesul general de gestionare a modificărilor din cadrul entității financiare, pentru a se asigura că toate modificările aduse sistemelor TIC sunt înregistrate, testate, evaluate, aprobate, puse în aplicare și verificate în mod controlat;

(f) dispun de politici adecvate și cuprinzătoare pentru corecții și actualizări.

În sensul literei (b), entitățile financiare concep infrastructura de conectare a rețelei într-un mod care permite întreruperea instantanee a acesteia și asigură compartimentarea și segmentarea sa, pentru a reduce la minimum și a preveni contagiunea, în special în cazul proceselor financiare interconectate.

În sensul literei (e), procesul de gestionare a modificărilor la nivelul TIC este aprobat de liniile de management corespunzătoare și dispune de protocoale specifice activate pentru modificări de urgență.

Articolul 9

Detectarea

1. Entitățile financiare dispun de mecanisme pentru detectarea rapidă a activităților anormale, în conformitate cu articolul 15, inclusiv a problemelor legate de performanța rețelei TIC și a incidentelor legate de TIC, precum și pentru identificarea tuturor punctelor unice semnificative de defecțiune posibile.

   Toate mecanismele de detectare menționate la primul paragraf sunt testate cu regularitate în conformitate cu articolul 22.

2. Mecanismele de detectare menționate la alineatul (1) permit niveluri multiple de control, definesc praguri de alertă și criterii de declanșare a proceselor de detectare a incidentelor legate de TIC și de răspuns la incidentele legate de TIC și instituie mecanisme de alertă automată pentru personalul relevant responsabil de răspunsul la incidentele legate de TIC.

3. Entitățile financiare alocă suficiente resurse și capacități, ținând seama în mod corespunzător de dimensiunea, activitatea și profilul lor de risc, pentru a monitoriza activitatea utilizatorilor, apariția anomaliilor TIC și a incidentelor legate de TIC, în special a atacurilor cibernetice.

4. Entitățile financiare menționate la articolul 2 alineatul (1) litera (l) dispun, în plus, de sisteme care pot verifica în mod eficace integralitatea rapoartelor de tranzacționare,

pot identifica omisiunile și erorile evidente și pot solicita retransmiterea acestor rapoarte în caz de erori de raportare.

Articolul 10

Răspunsul și recuperarea

1. Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 5 alineatul (1) și pe baza cerințelor de identificare prevăzute la articolul 7, entitățile financiare instituie o politică dedicată și cuprinzătoare de continuitate a activității bazate pe TIC, ca parte integrantă a politicii de continuitate a activității operaționale a entității financiare.

2. Entitățile financiare pun în aplicare politica de continuitate a activității bazate pe TIC menționată la alineatul (1) prin măsuri, planuri, proceduri și mecanisme specifice, adecvate și documentate, care vizează:

   (a) înregistrarea tuturor incidentelor legate de TIC;

   (b) asigurarea continuității funcțiilor critice ale entității financiare;

   (c) un răspuns rapid, adecvat și eficace la toate incidentele legate de TIC și soluționarea tuturor acestor incidente, în special – dar nu numai – atacurile cibernetice, într-un mod care să limiteze daunele și să acorde prioritate reluării activităților și acțiunilor de recuperare;

   (d) activarea fără întârziere a unor planuri specifice care permit aplicarea unor măsuri, procese și tehnologii de limitare, adecvate pentru fiecare tip de incident legat de TIC și prevenirea unor daune suplimentare, precum și proceduri de răspuns și de recuperare adaptate, stabilite în conformitate cu articolul 11;

   (e) estimarea impacturilor, a daunelor și a pierderilor preliminare;

   (f) stabilirea unor măsuri de comunicare și de gestionare a crizelor, care să asigure faptul că informațiile actualizate sunt transmise tuturor membrilor personalului intern relevant și părților interesate externe relevante, în conformitate cu articolul 13, și sunt totodată raportate autorităților competente, în conformitate cu articolul 17.

3. Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 5 alineatul (1), entitățile financiare pun în aplicare un plan asociat de recuperare a capabilităților TIC în caz de dezastru, care face obiectul unor audituri independente în cazul altor entități financiare decât microîntreprinderile.

4. Entitățile financiare instituie, mențin și testează periodic planuri adecvate privind continuitatea activității bazate pe TIC, în special în ceea ce privește funcțiile critice sau importante externalizate sau contractate prin acorduri cu furnizori terți de servicii TIC.

5. Ca parte a gestionării lor cuprinzătoare a riscurilor TIC, entitățile financiare:

   (a) testează politica de continuitate a activității bazate pe TIC și planul de recuperare a capabilităților TIC în caz de dezastru cel puțin o dată pe an și după modificări substanțiale aduse sistemelor TIC;

   (b) testează planurile de comunicare în situații de criză instituite în conformitate cu articolul 13.

În sensul literei (a), entitățile financiare, altele decât microîntreprinderile, includ în planurile de testare scenarii de atacuri cibernetice și de transfer între infrastructura TIC primară și capacitățile redundante, elementele de rezervă și instalațiile redundante necesare pentru a îndeplini obligațiile prevăzute la articolul 11.

Entitățile financiare își revizuiesc periodic politica de continuitate a activității bazate pe TIC și planul de recuperare a capabilităților TIC în caz de dezastru, ținând seama de rezultatele testelor efectuate în conformitate cu primul paragraf, precum și de recomandările care decurg din verificări de audit sau controale de supraveghere.

6. Entitățile financiare, altele decât microîntreprinderile, au o funcție de gestionare a crizelor, care, în cazul activării politicii lor de continuitate a activității bazate pe TIC sau a planului de recuperare a capabilităților TIC în caz de dezastru, stabilește proceduri clare de gestionare a comunicărilor interne și externe în situații de criză, în conformitate cu articolul 13.

7. Entitățile financiare păstrează evidența activităților înainte și în timpul evenimentelor perturbatoare atunci când se activează politica de continuitate a activității bazate pe TIC sau planul de recuperare a capabilităților TIC în caz de dezastru. Aceste evidențe sunt disponibile în orice moment.

8. Entitățile financiare menționate la articolul 2 alineatul (1) litera (f) furnizează autorităților competente copii ale rezultatelor testelor privind continuitatea activității bazate pe TIC sau ale unor exerciții similare realizate în perioada examinată.

9. Entitățile financiare, altele decât microîntreprinderile, raportează autorităților competente toate costurile și pierderile cauzate de perturbările TIC și de incidentele legate de TIC.

Articolul 11

Politici privind copiile de rezervă și metode de recuperare

1. Pentru a asigura redresarea sistemelor TIC cu un timp minim de indisponibilitate și o perturbare limitată, ca parte a cadrului lor de gestionare a riscurilor TIC, entitățile financiare elaborează:

   (a) o politică privind copiile de rezervă, care să precizeze sfera de acoperire a datelor care fac obiectul copierii de rezervă, precum și frecvența minimă a copierii de rezervă, pe baza caracterului critic al informațiilor sau a caracterului sensibil al datelor;

   (b) metode de recuperare.

2. Sistemele de rezervă demarează prelucrarea fără întârzieri nejustificate, cu excepția cazului în care demararea ar periclita securitatea rețelelor și a sistemelor informatice sau integritatea ori confidențialitatea datelor.

3. Atunci când recuperează date de rezervă pe baza sistemelor proprii, entitățile financiare utilizează sisteme TIC care au un mediu de operare diferit de cel principal, care nu este conectat direct cu acesta din urmă și care este protejat în mod securizat împotriva oricărui acces neautorizat sau a deteriorării TIC.

   În cazul entităților financiare menționate la articolul 2 alineatul (1) litera (g), planurile de recuperare permit recuperarea tuturor tranzacțiilor în momentul perturbării, pentru a permite contrapărții centrale să continue să opereze în condiții de siguranță și să finalizeze decontarea la data stabilită.

4. Entitățile financiare mențin capacități TIC redundante echipate cu resurse și funcționalități suficiente și adecvate pentru a acoperi nevoile operaționale.

5. Entitățile financiare enumerate la articolul 2 alineatul (1) litera (f) mențin sau se asigură că furnizorii lor terți de servicii TIC mențin cel puțin o unitate de prelucrare secundară, dotată cu resurse, capacități, funcționalități și resurse umane suficiente și adecvate pentru a acoperi nevoile operaționale.

   Unitatea de prelucrare secundară:

   (a) este situată la o distanță geografică față de unitatea de prelucrare principală pentru a se asigura că are un profil de risc distinct și pentru a preveni ca aceasta să fie afectată de evenimentul care a afectat unitatea de prelucrare principală;

   (b) este capabilă să asigure continuitatea serviciilor critice în mod identic cu unitatea de prelucrare principală sau să furnizeze nivelul serviciilor necesar pentru a se asigura că entitatea financiară își desfășoară operațiunile critice în conformitate cu obiectivele de recuperare;

   (c) este imediat accesibilă personalului entității financiare pentru a asigura continuitatea serviciilor critice în cazul în care unitatea de prelucrare principală a devenit indisponibilă.

6. Pentru a determina momentele de la care se pot reconstitui datele în urma unei întreruperi și intervalele maxime de recuperare în urma unei întreruperi pentru fiecare funcție, entitățile financiare iau în considerare impactul potențial global asupra eficienței pieței. Aceste obiective temporale asigură că, în scenarii extreme, nivelurile convenite ale serviciilor sunt respectate.

7. Atunci când se redresează în urma unui incident legat de TIC, entitățile financiare efectuează verificări multiple, inclusiv reconcilieri, pentru a se asigura că nivelul de integritate a datelor este cel mai ridicat. Aceste verificări se efectuează, de asemenea, atunci când sunt reconstituite date de la părțile interesate externe, pentru a se asigura că toate datele sunt coerente între sisteme.

Articolul 12

Învățăminte și evoluție

1. Entitățile financiare dispun de capacități și de personal adecvat în raport cu dimensiunea și cu profilurile lor de activitate și de risc, pentru a colecta informații cu privire la vulnerabilități, amenințări cibernetice și incidente legate de TIC, în special atacuri cibernetice, precum și pentru a analiza impacturile probabile ale acestora asupra rezilienței lor operaționale digitale.

2. Entitățile financiare instituie verificări ulterioare incidentelor legate de TIC, în urma unor perturbări TIC semnificative ale activităților lor de bază, analizând cauzele perturbării și identificând îmbunătățirile necesare pentru operațiunile TIC sau în cadrul politicii de continuitate a activității bazate pe TIC, la care se face referire la articolul 10.

   Atunci când pun în aplicare modificări, entitățile financiare, altele decât microîntreprinderile, comunică aceste modificări autorităților competente.

   Verificările ulterioare incidentelor legate de TIC la care se face referire la primul paragraf stabilesc dacă procedurile instituite au fost urmate și dacă măsurile luate au fost eficace, inclusiv în ceea ce privește:

(a) promptitudinea reacției la alertele de securitate și determinarea impactului și a gravității incidentelor legate de TIC;

(b) calitatea și rapiditatea efectuării analizelor judiciare;

(c) eficacitatea activării nivelurilor succesive de intervenție (*incident escalation)* în caz de incidente în cadrul entității financiare;

(d) eficacitatea comunicării interne și externe.

3. Învățămintele desprinse în urma testării privind reziliența operațională digitală, efectuată în conformitate cu articolele 23 și 24, precum și în urma incidentelor reale legate de TIC, în special a atacurilor cibernetice, alături de provocările întâmpinate la activarea planurilor privind continuitatea activității sau a planurilor de recuperare, împreună cu informațiile relevante schimbate cu contrapărțile și evaluate în timpul proceselor de supraveghere, sunt încorporate în mod corespunzător și continuu în procesul de evaluare a riscurilor TIC. Aceste constatări se traduc în revizuiri corespunzătoare ale componentelor relevante ale cadrului de gestionare a riscurilor TIC menționat la articolul 5 alineatul (1).

4. Entitățile financiare monitorizează eficacitatea punerii în aplicare a strategiei lor în materie de reziliență digitală, prevăzută la articolul 5 alineatul (9). Acestea cartografiază evoluția riscurilor TIC de-a lungul timpului, analizează frecvența, tipurile, magnitudinea și evoluția incidentelor legate de TIC, în special a atacurilor cibernetice și a modelelor lor, în vederea înțelegerii nivelului expunerii la riscurile TIC și a consolidării gradului de maturitate și de pregătire cibernetică a entității financiare.

5. Personalul de nivel superior din domeniul TIC raportează cel puțin o dată pe an către organul de conducere cu privire la rezultatele menționate la alineatul (3) și propune recomandări.

6. Entitățile financiare elaborează programe de sensibilizare cu privire la securitatea TIC și cursuri de formare în domeniul rezilienței operaționale digitale ca module obligatorii în cadrul programelor lor de formare a personalului. Acestea se aplică tuturor angajaților și personalului de conducere de nivel superior.

Entitățile financiare monitorizează evoluțiile tehnologice relevante în mod continuu, inclusiv pentru a înțelege posibilul impact al implementării unor astfel de noi tehnologii asupra cerințelor în materie de securitate TIC și a rezilienței operaționale digitale. Acestea trebuie să țină pasul cu cele mai recente procese de gestionare a riscurilor TIC, contracarând cu eficacitate formele actuale sau cele noi de atacuri cibernetice.

Articolul 13
Comunicarea

1. Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 5 alineatul (1), entitățile financiare instituie planuri de comunicare care să permită o informare responsabilă a clienților și a contrapărților, precum și a publicului, după caz, cu privire la incidentele legate de TIC sau la vulnerabilitățile majore.

2. Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 5 alineatul (1), entitățile financiare pun în aplicare politici de comunicare pentru personal și pentru părțile interesate externe. Politicile de comunicare pentru personal țin seama de necesitatea de a face distincția între personalul implicat în gestionarea

riscurilor TIC, în special la nivelul răspunsului și al recuperării, și personalul care trebuie să fie informat.

3. Cel puțin o persoană din entitate este însărcinată cu punerea în aplicare a strategiei de comunicare pentru incidentele legate de TIC și are rolul de purtător de cuvânt pentru public și mass-media în acest scop.

Articolul 14

Armonizarea în continuare a instrumentelor, metodelor, proceselor și politicilor de gestionare a riscurilor TIC

Autoritatea Bancară Europeană (ABE), Autoritatea Europeană pentru Valori Mobiliare și Piețe (ESMA) și Autoritatea Europeană de Asigurări și Pensii Ocupaționale (EIOPA), în consultare cu Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), elaborează proiecte de standarde tehnice de reglementare în următoarele scopuri:

(a) pentru a specifica alte elemente care să fie incluse în politicile, procedurile, protocoalele și instrumentele de securitate TIC menționate la articolul 8 alineatul (2), în scopul asigurării securității rețelelor, al asigurării unor garanții adecvate împotriva intruziunilor și a utilizării necorespunzătoare a datelor, al menținerii autenticității și integrității datelor, inclusiv tehnici criptografice, și al garantării unei transmiteri exacte și rapide a datelor fără perturbări majore;

(b) pentru a stabili modul în care politicile, procedurile și instrumentele de securitate TIC menționate la articolul 8 alineatul (2) includ controalele de securitate în sisteme de la început (securitate de la stadiul conceperii), permit ajustarea peisajului amenințărilor aflat în continuă schimbare și prevăd utilizarea tehnologiei de apărare în profunzime;

(c) pentru a aduce precizări suplimentare cu privire la tehnicile, metodele și protocoalele adecvate, menționate la articolul 8 alineatul (4) litera (b);

(d) pentru a dezvolta noi componente ale controalelor drepturilor de gestionare a accesului menționate la articolul 8 alineatul (4) litera (c) și politica privind resursele umane aferentă, care precizează drepturile de acces, procedurile de acordare și de revocare a drepturilor, monitorizarea comportamentului anormal în ceea ce privește riscurile TIC prin intermediul unor indicatori adecvați, inclusiv pentru modelele de utilizare a rețelei, orele, activitatea IT și dispozitivele necunoscute;

(e) pentru a dezvolta în continuare elementele specificate la articolul 9 alineatul (1) care permit detectarea promptă a activităților anormale și criteriile menționate la articolul 9 alineatul (2) care determină procesele de detectare și de răspuns la incidente legate de TIC;

(f) pentru a aduce precizări suplimentare cu privire la componentele politicii de continuitate a activității bazate pe TIC, menționată la articolul 10 alineatul (1);

(g) pentru a aduce precizări suplimentare cu privire la testarea planurilor privind continuitatea activității bazate pe TIC menționate la articolul 10 alineatul (5), pentru a se asigura că ține seama în mod corespunzător de scenariile în care calitatea furnizării unei funcții critice sau importante se deteriorează până la un nivel inacceptabil sau eșuează, precum și că ia în considerare în mod corespunzător impactul potențial al insolvenței sau al altor disfuncționalități ale

oricărui furnizor terț de servicii TIC relevant și, dacă este cazul, riscurile politice din jurisdicțiile furnizorilor respectivi;

(h) pentru a aduce precizări suplimentare cu privire la componentele planului de recuperare a capabilităților TIC în caz de dezastru, menționat la articolul 10 alineatul (3).

ABE, ESMA și EIOPA înaintează Comisiei aceste proiecte de standarde tehnice de reglementare până la [*JO: a se introduce data - 1 an de la data intrării în vigoare*].

Se deleagă Comisiei competența de a adopta standardele tehnice de reglementare menționate la primul paragraf în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și, respectiv, (UE) nr. 1095/2010.

CAPITOLUL III

INCIDENTE LEGATE DE TIC

GESTIONAREA, CLASIFICAREA și RAPORTAREA

Articolul 15

Procesul de gestionare a incidentelor legate de TIC

1. Entitățile financiare stabilesc și pun în aplicare un proces de gestionare a incidentelor legate de TIC pentru a detecta, a gestiona și a notifica incidentele legate de TIC și instituie indicatori de avertizare timpurie care să funcționeze ca alerte.

2. Entitățile financiare instituie proceduri adecvate pentru a garanta o monitorizare, o tratare și o urmărire consecvente și integrate a incidentelor legate de TIC, vizând a asigura identificarea și eradicarea cauzelor lor principale, astfel încât să se prevină apariția unor astfel de incidente.

3. Procesul de gestionare a incidentelor legate de TIC menționat la alineatul (1):

   (a) stabilește proceduri pentru identificarea, urmărirea, înregistrarea, indicarea categoriei și clasificarea incidentelor legate de TIC în funcție de prioritatea lor și de gravitatea și de caracterul critic al serviciilor afectate, în conformitate cu criteriile menționate la articolul 16 alineatul (1);

   (b) alocă roluri și responsabilități care trebuie activate pentru diferite tipuri și scenarii de incidente legate de TIC;

   (c) stabilește planuri pentru comunicarea cu personalul, cu părțile interesate externe și cu mass-media, în conformitate cu articolul 13, și pentru notificarea clienților, proceduri interne de activare a nivelurilor succesive de intervenție (*escalation*), inclusiv în cazul unor plângeri din partea clienților legate de TIC, precum și pentru furnizarea de informații entităților financiare care acționează în calitate de contrapărți, după caz;

   (d) asigură că incidentele majore legate de TIC sunt raportate conducerii superioare relevante și informează organul de conducere cu privire la incidente majore legate de TIC, explicând impactul, răspunsul și controalele suplimentare care urmează să fie instituite ca urmare a incidentelor legate de TIC;

(e) stabilește proceduri de răspuns la incidentele legate de TIC în vederea atenuării impactului și a asigurării faptului că serviciile devin operaționale și sigure în timp util.

Articolul 16

Clasificarea incidentelor legate de TIC

1. Entitățile financiare clasifică incidentele legate de TIC și determină impactul acestora pe baza următoarelor criterii:

(a) numărul de utilizatori sau de contrapărți financiare afectate de perturbarea cauzată de incidentul legat de TIC și dacă incidentul legat de TIC a avut impact asupra reputației;

(b) durata incidentului legat de TIC, inclusiv perioada de indisponibilitate a serviciului;

(c) întinderea geografică în ceea ce privește zonele afectate de incidentul legat de TIC, în special dacă acesta afectează mai mult de două state membre;

(d) pierderile de date generate de un incident legat de TIC, cum ar fi pierderea integrității, a confidențialității sau a disponibilității;

(e) gravitatea impactului incidentului legat de TIC asupra sistemelor TIC ale entității financiare;

(f) caracterul critic al serviciilor afectate, inclusiv al tranzacțiilor și operațiunilor entității financiare;

(g) impactul economic al incidentului legat de TIC, atât în termeni absoluți, cât și relativi.

2. Prin intermediul Comitetului comun al AES (denumit în continuare „Comitetul comun”) și după consultarea Băncii Centrale Europene (BCE) și a ENISA, AES elaborează proiecte comune de standarde tehnice de reglementare aducând precizări suplimentare cu privire la următoarele:

(a) criteriile menționate la alineatul (1), inclusiv pragurile de semnificație pentru determinarea incidentelor majore legate de TIC care fac obiectul obligației de raportare prevăzute la articolul 17 alineatul (1);

(b) criteriile care trebuie aplicate de autoritățile competente în scopul evaluării relevanței incidentelor majore legate de TIC pentru jurisdicțiile altor state membre, precum și detalii ale rapoartelor privind incidentele legate de TIC care trebuie să fie comunicate altor autorități competente în temeiul articolului 17 punctele 5 și 6.

3. Atunci când elaborează proiectele comune de standarde tehnice de reglementare menționate la alineatul (2), AES țin seama de standardele internaționale, precum și de specificațiile elaborate și publicate de ENISA, inclusiv, după caz, de specificațiile pentru alte sectoare economice.

AES transmit Comisiei respectivele proiecte comune de standarde tehnice de reglementare până la [*OP: a se introduce data - 1 an de la data intrării în vigoare*].

Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la alineatul (2) în conformitate cu

articolele 10-14 din Regulamentul (UE) nr. 1093/2010, (UE) nr. 1094/2010 și, respectiv, (UE) nr. 1095/2010.

Articolul 17

Raportarea incidentelor majore legate de TIC

1. Entitățile financiare raportează autorității competente relevante, menționată la articolul 41, incidentele majore legate de TIC, în termenele prevăzute la alineatul (3).

   În sensul primului paragraf, entitățile financiare elaborează, după colectarea și analizarea tuturor informațiilor relevante, un raport privind incidentele, utilizând modelul menționat la articolul 18, și îl transmite autorității competente.

   Raportul include toate informațiile necesare autorității competente pentru a determina importanța incidentului major legat de TIC și a evalua posibilele efecte transfrontaliere.

2. În cazul în care un incident major legat de TIC are sau poate avea un impact asupra intereselor financiare ale utilizatorilor și clienților serviciilor, entitățile financiare informează, fără întârzieri nejustificate, utilizatorii și clienții serviciilor lor cu privire la incidentul major legat de TIC și le aduc la cunoștință cât mai curând posibil toate măsurile care au fost luate pentru a atenua efectele nefavorabile ale unui astfel de incident.

3. Entitățile financiare transmit autorității competente menționate la articolul 41:

   (a) o notificare inițială, fără întârziere, dar nu mai târziu de sfârșitul zilei lucrătoare sau, în cazul unui incident major legat de TIC care a avut loc cu mai puțin de 2 ore înainte de încheierea zilei lucrătoare, nu mai târziu de 4 ore de la începutul următoarei zile lucrătoare sau, în cazul în care nu sunt disponibile canale de raportare, de îndată ce acestea devin disponibile;

   (b) un raport intermediar, în termen de cel mult 1 săptămână de la notificarea inițială menționată la litera (a), urmat, după caz, de notificări actualizate de fiecare dată când este disponibilă o actualizare relevantă a statutului, precum și la solicitarea specifică a autorității competente;

   (c) un raport final, atunci când analiza cauzelor principale a fost finalizată, indiferent dacă măsurile de atenuare au fost sau nu deja puse în aplicare, precum și atunci când cifrele efective ale impactului sunt disponibile pentru a înlocui estimările, dar nu mai târziu de o lună de la data la care a fost trimis raportul inițial.

4. Entitățile financiare pot delega obligațiile de raportare prevăzute la prezentul articol către un furnizor terț de servicii numai dacă delegarea este aprobată de autoritatea competentă relevantă menționată la articolul 41.

5. La primirea raportului menționat la alineatul (1), autoritatea competentă transmite, fără întârzieri nejustificate, detalii referitoare la incident, către:

   (a) ABE, ESMA sau EIOPA, după caz;

   (b) BCE, după caz, pentru entitățile financiare menționate la articolul 2 alineatul (1) literele (a), (b) și (c); și

   (c) punctul unic de contact desemnat în temeiul articolului 8 din Directiva (UE) 2016/1148.

6. ABE, ESMA sau EIOPA și BCE evaluează relevanța incidentului major legat de TIC pentru alte autorități publice relevante și le notifică în consecință, în cel mai scurt timp posibil. BCE notifică membrilor Sistemului European al Băncilor Centrale aspectele relevante pentru sistemul de plată. Pe baza notificării respective, autoritățile competente iau, după caz, toate măsurile necesare pentru protejarea stabilității imediate a sistemului financiar.

Articolul 18

Armonizarea conținutului rapoartelor și a modelelor de rapoarte

1. AES, prin intermediul Comitetului comun și după consultarea ENISA și a BCE, elaborează:

   (a) proiecte comune de standarde tehnice de reglementare pentru:

      (1) a stabili conținutul rapoartelor în cazul incidentelor majore legate de TIC;

      (2) a aduce precizări suplimentare cu privire la condițiile în care entitățile financiare pot delega unui furnizor terț de servicii, cu aprobarea prealabilă a autorității competente, obligațiile de raportare prevăzute în prezentul capitol;

   (b) proiecte comune de standarde tehnice de punere în aplicare în vederea stabilirii formularelor, modelelor și procedurilor standard pentru raportarea de către entitățile financiare a unui incident major legat de TIC.

   AES transmit Comisiei proiectele comune de standarde tehnice de reglementare menționate la alineatul (1) litera (a) și proiectele comune de standarde tehnice de punere în aplicare menționate la alineatul (1) litera (b), până la xx 202x [*OP: a se introduce data - 1 an de la data intrării în vigoare*].

   Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare comune menționate la alineatul (1) litera (a) în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1095/2010 și, respectiv, (UE) nr. 1094/2010.

   Se deleagă Comisiei competența de a adopta standardele tehnice de punere în aplicare comune menționate la alineatul (1) litera (b) în conformitate cu articolul 15 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1095/2010 și, respectiv, (UE) nr. 1094/2010.

Articolul 19

Centralizarea raportării incidentelor majore legate de TIC

1. AES elaborează, prin intermediul Comitetului comun și în consultare cu BCE și ENISA, un raport comun de evaluare a fezabilității centralizării în continuare a raportării incidentelor prin crearea unei platforme unice a UE pentru raportarea incidentelor majore legate de TIC de către entitățile financiare. Raportul analizează modalitățile de facilitare a fluxului raportării incidentelor legate de TIC, de reducere a costurilor asociate și de susținere a analizelor tematice în vederea consolidării convergenței în materie de supraveghere.

2. Raportul menționat la alineatul (1) cuprinde cel puțin următoarele elemente:

   (a) condițiile prealabile pentru instituirea unei astfel de platforme a UE;

(b) beneficiile, limitările și riscurile posibile;

(c) elemente ale gestionării operaționale;

(d) condițiile de participare;

(e) modalitățile de accesare a platformei UE de către entitățile financiare și autoritățile naționale competente;

(f) o evaluare preliminară a costurilor financiare implicate de instituirea platformei operaționale care sprijină platforma UE, inclusiv expertiza necesară.

3. AES transmit raportul menționat la alineatul (1) Comisiei, Parlamentului European și Consiliului până la xx 202x [*JO: a se introduce data - 3 ani de la data intrării în vigoare*].

Articolul 20

Feedback privind supravegherea

1. La primirea unui raport, astfel cum se menționează la articolul 17 alineatul (1), autoritatea competentă confirmă primirea notificării și furnizează entității financiare, în cel mai scurt timp posibil, toate observațiile sau îndrumările necesare, în special pentru a discuta măsurile de remediere la nivelul entității sau modalitățile de a reduce la minimum impactul negativ la nivelul tuturor sectoarelor.

2. Prin intermediul Comitetului comun, AES raportează anual, în mod anonim și agregat, cu privire la notificările incidentelor legate de TIC primite de la autoritățile competente, stabilind cel puțin numărul incidentelor majore legate de TIC, natura acestora, impactul asupra operațiunilor entităților financiare sau ale clienților, costurile și măsurile de remediere luate.

AES emit avertismente și elaborează statistici la nivel înalt pentru a sprijini evaluările privind amenințările și vulnerabilitățile din perspectiva TIC.

CAPITOLUL IV

TESTAREA REZILIENȚEI OPERAȚIONALE DIGITALE

Articolul 21

Cerințe generale pentru efectuarea testării rezilienței operaționale digitale

1. În scopul evaluării nivelului de pregătire pentru incidentele legate de TIC, al identificării punctelor slabe, a deficiențelor sau a lacunelor în ceea ce privește reziliența operațională digitală și al punerii în aplicare prompte a măsurilor corective, entitățile financiare stabilesc, mențin și revizuiesc, ținând seama în mod corespunzător de dimensiunea și de profilurile lor de activitate și de risc, un program solid și cuprinzător de testare a rezilienței operaționale digitale ca parte integrantă a cadrului de gestionare a riscurilor TIC menționat la articolul 5.

2. Programul de testare a rezilienței operaționale digitale include o serie de evaluări, teste, metodologii, practici și instrumente care trebuie aplicate în conformitate cu dispozițiile prevăzute la articolele 22 și 23.

3. Entitățile financiare urmează o abordare bazată pe riscuri în cadrul programului de testare a rezilienței operaționale digitale menționat la alineatul (1), ținând seama de

evoluția peisajului riscurilor TIC, de orice riscuri specifice la care este sau ar putea fi expusă entitatea financiară, de caracterul critic al activelor informaționale și al serviciilor furnizate, precum și de orice alt factor pe care entitatea financiară îl consideră adecvat.

4. Entitățile financiare se asigură că testele sunt efectuate de părți independente, interne sau externe.

5. Entitățile financiare stabilesc proceduri și politici care să prioritizeze, să clasifice și să remedieze toate chestiunile recunoscute pe parcursul desfășurării testelor și stabilesc metodologii de validare internă pentru a se asigura că toate punctele slabe, deficiențele sau lacunele identificate sunt abordate integral.

6. Entitățile financiare testează toate sistemele și aplicațiile TIC esențiale cel puțin o dată pe an.

Articolul 22

Testarea instrumentelor și sistemelor TIC

1. Programul de testare a rezilienței operaționale digitale, menționat la articolul 21, asigură efectuarea unei game complete de teste adecvate, inclusiv evaluări și examinări ale vulnerabilității, analize ale surselor deschise, evaluări ale securității rețelei, analize ale lacunelor, verificări ale securității fizice, chestionare și soluții de scanare a programelor software, evaluări ale codului sursă atunci când este fezabil, teste bazate pe scenarii, teste de compatibilitate, teste de performanță, teste integrale (*end-to-end*) sau teste de penetrare.

2. Entitățile financiare enumerate la articolul 2 alineatul (1) literele (f) și (g) efectuează evaluări ale vulnerabilității înainte de utilizarea sau reutilizarea unor servicii noi sau existente care sprijină funcțiile, aplicațiile și componentele de infrastructură critice ale entității financiare.

Articolul 23

Testarea avansată a instrumentelor, sistemelor și proceselor TIC cu ajutorul testelor de penetrare bazate pe amenințări

1. Entitățile financiare identificate în conformitate cu alineatul (4) efectuează, cel puțin o dată la 3 ani, o testare avansată cu ajutorul testelor de penetrare bazate pe amenințări.

2. Testele de penetrare bazate pe amenințări acoperă cel puțin funcțiile și serviciile critice ale unei entități financiare și sunt realizate pe sistemele de producție în timp real care sprijină astfel de funcții. Domeniul de aplicare exact al testelor de penetrare bazate pe amenințări, fondate pe evaluarea funcțiilor și serviciilor critice, se stabilește de către entitățile financiare și este validat de către autoritățile competente.

   În sensul primului paragraf, entitățile financiare identifică toate procesele, sistemele și tehnologiile TIC subiacente relevante, care sprijină funcțiile și serviciile critice, inclusiv funcțiile și serviciile externalizate sau contractate unor furnizori terți de servicii TIC.

   În cazul în care furnizorii terți de servicii TIC sunt incluși în domeniul de aplicare al testelor de penetrare bazate pe amenințări, entitatea financiară ia măsurile necesare pentru a asigura participarea acestor furnizori.

Entitățile financiare efectuează controale eficace ale gestionării riscurilor pentru a reduce riscurile unui impact potențial asupra datelor și riscurile de deteriorare a activelor și de perturbare a serviciilor sau a operațiunilor critice la nivelul entității financiare înseși, al contrapărților acesteia sau al sectorului financiar.

La sfârșitul testului, după ce s-a convenit cu privire la rapoarte și planurile de remediere, entitatea financiară și entitățile externe care efectuează testele furnizează autorității competente documentația care confirmă faptul că testul de penetrare bazat pe amenințări a fost efectuat în conformitate cu cerințele. Autoritățile competente validează documentația și eliberează o adeverință.

3. Entitățile financiare contractează testeri în conformitate cu articolul 24 în scopul efectuării unui test de penetrare bazat pe amenințări.

Autoritățile competente identifică entitățile financiare care să realizeze teste de penetrare bazate pe amenințări, în mod proporțional cu dimensiunea, amploarea, activitatea și profilul general de risc ale entității financiare, pe baza evaluării următoarelor elemente:

(a) factorii legați de impact, în special caracterul critic al serviciilor furnizate și al activităților întreprinse de entitatea financiară;

(b) posibilele preocupări legate de stabilitatea financiară, inclusiv caracterul sistemic al entității financiare la nivel național sau la nivelul Uniunii, după caz;

(c) profilul specific de risc TIC, nivelul de maturitate a entității financiare din perspectiva TIC sau caracteristicile tehnologice implicate.

4. După consultarea BCE și ținând seama de cadrele relevante din Uniune, care se aplică testelor de penetrare bazate pe date operative, ABE, ESMA și EIOPA elaborează proiecte de standarde tehnice de reglementare pentru a aduce precizări suplimentare cu privire la:

(a) criteriile utilizate în scopul aplicării alineatului (6) de la prezentul articol;

(b) cerințele privind:

(a) domeniul de aplicare al testului de penetrare bazat pe amenințări menționat la alineatul (2) de la prezentul articol;

(b) metodologia de testare și abordarea de urmat pentru fiecare fază specifică a procesului de testare;

(c) rezultatele, încheierea și etapele procesului de remediere aferente testării;

(c) tipul de cooperare în materie de supraveghere necesară pentru punerea în aplicare a testelor de penetrare bazate pe amenințări în contextul entităților financiare care operează în mai multe state membre, pentru a permite un nivel adecvat de implicare din perspectiva supravegherii și o aplicare flexibilă astfel încât să se țină seama de specificitățile subsectoarelor financiare sau ale piețelor financiare locale.

AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la [*JO: A se introduce data: 2 luni înainte de data intrării în vigoare*].

Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la al doilea paragraf în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1095/2010 și, respectiv, (UE) nr. 1094/2010.

Articolul 24

Cerințe pentru entitățile care efectuează testele

1. Entitățile financiare utilizează, în scopul efectuării testelor de penetrare bazate pe amenințări, numai testeri care:

   (a) sunt cele mai adecvate și de cea mai înaltă reputație;

   (b) dețin capacități tehnice și organizatorice și demonstrează expertiză specifică în ceea ce privește datele operative privind amenințările, testele de penetrare sau testele bazate pe „echipa roșie”;

   (c) sunt certificate de un organism de acreditare dintr-un stat membru sau aderă la coduri de conduită sau cadre etice oficiale;

   (d) în cazul entităților externe care efectuează testele, oferă o asigurare independentă sau un raport de audit în ceea ce privește gestionarea solidă a riscurilor asociate cu executarea testelor de penetrare bazate pe amenințări, inclusiv protecția adecvată a informațiilor confidențiale ale entității financiare și măsurile reparatorii pentru riscurile legate de activitățile entității financiare;

   (e) în cazul entităților externe care efectuează testele, sunt acoperite în mod corespunzător și în totalitate de asigurările de răspundere civilă profesională relevante, inclusiv împotriva riscurilor de abatere și neglijență.

2. Entitățile financiare asigură că acordurile încheiate cu testeri externi necesită o gestionare solidă a rezultatelor testelor de penetrare bazate pe amenințări și că orice prelucrare a acestora, inclusiv orice generare, elaborare, stocare, agregare, raportare, comunicare sau distrugere, nu creează riscuri pentru entitatea financiară.

CAPITOLUL V

GESTIONAREA RISCURILOR TIC GENERATE DE PĂRȚI TERȚE

SECȚIUNEA I

PRINCIPII-CHEIE PENTRU O GESTIONARE SOLIDĂ A RISCURILOR TIC GENERATE DE PĂRȚI TERȚE

Articolul 25

Principii generale

Entitățile financiare gestionează riscurile TIC generate de părți terțe ca o componentă integrantă a riscurilor TIC în cadrul lor de gestionare a riscurilor TIC și în conformitate cu următoarele principii:

1. Entitățile financiare care au instituit acorduri contractuale pentru utilizarea serviciilor TIC în scopul desfășurării operațiunilor lor rămân în orice moment pe deplin responsabile de respectarea și de îndeplinirea tuturor obligațiilor care decurg din prezentul regulament și din legislația aplicabilă în domeniul serviciilor financiare.

2. Gestionarea de către entitățile financiare a riscurilor TIC generate de părți terțe este pusă în aplicare din perspectiva principiului proporționalității, luând în considerare:

(a) amploarea, complexitatea și importanța dependențelor legate de TIC;

(b) riscurile care decurg din acordurile contractuale privind utilizarea serviciilor TIC încheiate cu furnizori terți de servicii TIC, ținând seama de caracterul critic sau importanța serviciului, procesului sau funcției respective, precum și de impactul potențial asupra continuității și calității serviciilor și activităților financiare, la nivel individual și la nivel de grup.

3. Ca parte a cadrului lor de gestionare a riscurilor TIC, entitățile financiare adoptă și revizuiesc periodic o strategie privind riscurile TIC generate de părți terțe, ținând seama de strategia pentru furnizori multipli, menționată la articolul 5 alineatul (9) litera (g). Această strategie include o politică privind utilizarea serviciilor TIC furnizate de furnizori terți de servicii TIC și se aplică pe o bază individuală și, după caz, pe o bază subconsolidată și consolidată. Organul de conducere reexaminează periodic riscurile identificate în ceea ce privește externalizarea funcțiilor critice sau importante.

4. Ca parte a cadrului lor de gestionare a riscurilor TIC, entitățile financiare mențin și actualizează la nivel de entitate și la nivel subconsolidat și consolidat un registru de informații în legătură cu toate acordurile contractuale privind utilizarea serviciilor TIC furnizate de furnizori terți de servicii TIC.

Acordurile contractuale menționate la primul paragraf sunt documentate în mod corespunzător, făcându-se distincția între cele care acoperă funcții critice sau importante și cele care nu acoperă astfel de funcții.

Entitățile financiare raportează cel puțin o dată pe an autorităților competente informații privind numărul de noi acorduri privind utilizarea serviciilor TIC, categoriile de furnizori terți de servicii TIC, tipurile de acorduri contractuale și serviciile și funcțiile care sunt furnizate.

Entitățile financiare pun la dispoziția autorității competente, la cerere, registrul complet de informații sau, după caz, secțiuni specifice din acesta, împreună cu orice informații considerate necesare pentru a permite supravegherea eficace a entității financiare.

Entitățile financiare informează autoritatea competentă în timp util cu privire la contractarea planificată a unor funcții critice sau importante, precum și atunci când o funcție a devenit critică sau importantă.

5. Înainte de a încheia un acord contractual privind utilizarea serviciilor TIC, entitățile financiare:

(a) evaluează dacă acordul contractual acoperă o funcție critică sau importantă;

(b) evaluează dacă sunt îndeplinite condițiile pentru contractare din perspectiva supravegherii;

(c) identifică și evaluează toate riscurile relevante legate de acordul contractual, inclusiv posibilitatea ca astfel de acorduri contractuale să contribuie la consolidarea riscului de concentrare a serviciilor TIC;

(d) efectuează toate procesele de diligență cu privire la potențialii furnizori terți de servicii TIC și asigură, pe parcursul proceselor de selecție și evaluare, că furnizorul terț de servicii TIC este adecvat;

(e) identifică și evaluează conflictele de interese pe care acordul contractual le poate cauza.

6. Entitățile financiare pot încheia acorduri contractuale numai cu furnizori terți de servicii TIC care respectă standardele înalte, adecvate și de ultimă dată privind siguranța informațiilor.

7. În exercitarea drepturilor de acces, de inspecție și de audit cu privire la furnizorul terț de servicii TIC, entitățile financiare stabilesc în prealabil, utilizând o abordare bazată pe riscuri, frecvența auditurilor și a inspecțiilor, precum și domeniile care urmează să fie auditate prin aderarea la standardele de audit acceptate de comun acord, în concordanță cu instrucțiunile de supraveghere privind utilizarea și integrarea unor astfel de standarde de audit.

   În cazul acordurilor contractuale care implică un nivel ridicat de complexitate tehnologică, entitatea financiară verifică dacă auditorii, atât cei interni, cât și grupurile de auditori sau auditorii externi, dețin competențele și cunoștințele corespunzătoare pentru a efectua în mod eficace auditurile și evaluările relevante.

8. Entitățile financiare asigură că acordurile contractuale privind utilizarea serviciilor TIC sunt reziliate cel puțin în următoarele circumstanțe:

   (a) încălcarea de către furnizorul terț de servicii TIC a actelor cu putere de lege, a reglementărilor sau a clauzelor contractuale aplicabile;

   (b) circumstanțele identificate pe parcursul monitorizării riscurilor TIC generate de părți terțe, care sunt considerate capabile să modifice îndeplinirea funcțiilor asigurate prin acordul contractual, inclusiv modificările semnificative care afectează acordul sau situația furnizorului terț de servicii TIC;

   (c) deficiențele demonstrate ale furnizorului terț de servicii TIC în gestionarea sa generală a riscurilor TIC și, în special, în modul în care asigură securitatea și integritatea datelor confidențiale, cu caracter personal sau sensibile din alt punct de vedere ori a informațiilor fără caracter personal;

   (d) circumstanțele în care autoritatea competentă nu mai poate supraveghea în mod eficace entitatea financiară, ca urmare a angajamentului contractual respectiv.

9. Entitățile financiare instituie strategii de ieșire pentru a ține seama de riscurile care pot apărea la nivelul furnizorului terț de servicii TIC, în special o posibilă deficiență a acestuia din urmă, o deteriorare a calității funcțiilor furnizate, orice perturbare a activității cauzată de furnizarea necorespunzătoare sau defectuoasă a serviciilor sau de riscuri semnificative care decurg din utilizarea adecvată și continuă a funcției.

   Entitățile financiare se asigură că pot să rezilieze acordurile contractuale fără:

   (a) perturbarea activităților lor comerciale;

   (b) limitarea respectării cerințelor în materie de reglementare;

   (c) afectarea continuității și calității furnizării serviciilor către clienți.

   Planurile de ieșire trebuie să fie cuprinzătoare, documentate și, după caz, testate în mod suficient.

   Entitățile financiare identifică soluții alternative și dezvoltă planuri de tranziție care să le permită să elimine funcțiile contractate și datele relevante de la furnizorul terț de servicii TIC și să le transfere în condiții de siguranță și în integralitatea lor către furnizori alternativi sau să le reintegreze în sistemul propriu.

Entitățile financiare iau măsurile adecvate pentru situațiile neprevăzute astfel încât să păstreze continuitatea activității în toate situațiile menționate în primul paragraf.

10. AES elaborează, prin intermediul Comitetului comun, proiecte de standarde tehnice de punere în aplicare pentru a stabili modelele standard pentru registrul de informații menționat la alineatul (4).

AES transmit Comisiei aceste proiecte de standarde tehnice de punere în aplicare până la [*JO: A se introduce data: 1 an de la data intrării în vigoare a prezentului regulament*].

Se conferă Comisiei competența de a adopta standardele tehnice de punere în aplicare menționate la primul paragraf în conformitate cu articolul 15 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1095/2010 și, respectiv, (UE) nr. 1094/2010.

11. AES elaborează, prin intermediul Comitetului comun, proiecte de standarde de reglementare:

(a) pentru a aduce noi precizări privind conținutul detaliat al politicii menționate la alineatul (3) în legătură cu acordurile contractuale privind utilizarea serviciilor TIC furnizate de furnizori terți de servicii TIC, prin trimitere la principalele etape ale ciclului de viață a respectivelor acorduri privind utilizarea serviciilor TIC;

(b) tipurile de informații care trebuie incluse în registrul de informații menționat la alineatul (4).

AES transmit Comisiei aceste proiecte comune de standarde tehnice de reglementare până la [*OP: a se introduce data - 1 an de la data intrării în vigoare*].

Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la al doilea paragraf în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1095/2010 și, respectiv, (UE) nr. 1094/2010.

Articolul 26

Evaluarea preliminară a riscului de concentrare a serviciilor TIC, precum și a unor noi acorduri de subcontractare a serviciilor externalizate

1. La identificarea și evaluarea riscului de concentrare a serviciilor TIC menționat la articolul 25 alineatul (5) litera (c), entitățile financiare țin seama de aspectul dacă încheierea unui acord contractual în legătură cu serviciile TIC ar conduce la oricare dintre următoarele situații:

(a) contractarea cu un furnizor terț de servicii TIC care nu este ușor de înlocuit; sau

(b) instituirea unor acorduri contractuale multiple cu privire la furnizarea de servicii TIC cu același furnizor terț de servicii TIC sau cu furnizori terți de servicii TIC strâns interconectați.

Entitățile financiare evaluează beneficiile și costurile soluțiilor alternative, cum ar fi utilizarea unor furnizori terți de servicii TIC diferiți, luând în considerare dacă și în ce mod soluțiile avute în vedere corespund nevoilor și obiectivelor operaționale stabilite în strategia lor privind reziliența digitală.

2. În cazul în care acordul contractual privind utilizarea serviciilor TIC include posibilitatea ca un furnizor terț de servicii TIC să subcontracteze în continuare o funcție critică sau importantă către alți furnizori terți de servicii TIC, entitățile financiare evaluează beneficiile și riscurile care pot apărea în legătură cu o astfel de potențială subcontractare, în special în cazul unui subcontractant TIC stabilit într-o țară terță.

   În cazul în care acordurile contractuale privind utilizarea serviciilor TIC sunt încheiate cu un furnizor terț de servicii TIC stabilit într-o țară terță, entitățile financiare consideră ca fiind relevanți cel puțin următorii factori:

   (a) respectarea normelor privind protecția datelor;

   (b) aplicarea efectivă a legislației;

   (c) dispozițiile din legea insolvenței care s-ar aplica în eventualitatea falimentului furnizorului terț de servicii TIC;

   (d) orice constrângeri care ar putea apărea în legătură cu recuperarea urgentă a datelor entității financiare.

   Entitățile financiare evaluează dacă și în ce mod lanțurile lungi sau complexe de subcontractare pot avea un impact asupra capacității lor de a monitoriza pe deplin funcțiile contractate și asupra capacității autorității competente de a supraveghea efectiv entitatea financiară din acest punct de vedere.

Articolul 27

Dispoziții contractuale esențiale

1. Drepturile și obligațiile care revin entității financiare și furnizorului terț de servicii TIC sunt clar atribuite și definite în scris. Contractul complet, care include acordurile privind nivelul serviciilor, este confirmat într-un document scris aflat la dispoziția părților, pe suport de hârtie sau într-un format accesibil și care poate fi descărcat.

2. Acordurile contractuale privind utilizarea serviciilor TIC includ cel puțin următoarele:

   (a) o descriere clară și completă a tuturor funcțiilor și serviciilor care urmează să fie furnizate de furnizorul terț de servicii TIC, indicând dacă este permisă subcontractarea unei funcții critice sau importante sau a unor părți semnificative ale acesteia și, în caz afirmativ, condițiile aplicabile acestei subcontractări;

   (b) locațiile în care urmează să fie furnizate funcțiile și serviciile contractate sau subcontractate și în care urmează să fie prelucrate datele, inclusiv locul stabilit pentru stocare, precum și cerința ca furnizorul terț de servicii TIC să informeze entitatea financiară în cazul în care are în vedere modificarea acestor locații;

   (c) dispoziții privind accesibilitatea, disponibilitatea, integritatea, securitatea și protecția datelor cu caracter personal și asigurarea accesului, a recuperării și a returnării într-un format ușor accesibil a datelor cu caracter personal și a celor fără caracter personal prelucrate de entitatea financiară în caz de insolvență, de rezoluție sau de întrerupere a activității furnizorului terț de servicii TIC;

   (d) descrieri complete ale nivelului serviciului, inclusiv actualizări și revizuiri ale acestora, precum și obiective cantitative și calitative precise privind performanța în limitele nivelurilor convenite ale serviciilor, pentru a permite o

monitorizare eficace de către entitatea financiară și aplicarea, fără întârzieri nejustificate, a măsurilor corective adecvate atunci când nu sunt asigurate nivelurile convenite ale serviciilor;

(e) perioade de preaviz și obligații de raportare către entitatea financiară pentru furnizorul terț de servicii TIC, inclusiv notificarea oricărei evoluții care ar putea avea un impact semnificativ asupra capacității furnizorului terț de servicii TIC de a îndeplini în mod eficace funcții critice sau importante, în concordanță cu nivelurile convenite ale serviciului;

(f) obligația furnizorului terț de servicii TIC de a oferi asistență în cazul unui incident TIC fără costuri suplimentare sau la un cost stabilit *ex ante*;

(g) cerințe ca furnizorul terț de servicii TIC să pună în aplicare și să testeze planuri pentru situații neprevăzute și să dispună de măsuri, instrumente și politici în materie de securitate a TIC care să garanteze în mod adecvat furnizarea în condiții de siguranță a serviciilor de către entitatea financiară, în concordanță cu cadrul său de reglementare;

(h) dreptul de a monitoriza în permanență performanța furnizorului terț de servicii TIC, care include:

(i) dreptul de acces, de inspecție și de audit de către entitatea financiară sau de către o parte terță desemnată, precum și dreptul de a lua copii ale documentelor relevante, a căror exercitare efectivă nu este împiedicată sau limitată de alte acorduri contractuale sau politici de punere în aplicare;

(ii) dreptul de a conveni asupra unor niveluri de asigurare alternative în cazul în care sunt afectate drepturile altor clienți;

(iii) angajamentul de a coopera pe deplin în timpul inspecțiilor la fața locului efectuate de entitatea financiară și detalii privind domeniul de aplicare, modalitățile și frecvența auditurilor la distanță;

(i) obligația furnizorului terț de servicii TIC de a coopera pe deplin cu autoritățile competente și cu autoritățile de rezoluție ale entității financiare, inclusiv cu persoanele numite de acestea;

(j) drepturile de reziliere și perioada minimă conexă de notificare pentru încetarea contractului, în conformitate cu așteptările autorităților competente;

(k) strategii de ieșire, în special stabilirea unei perioade de tranziție adecvate obligatorii:

(a) în cursul căreia furnizorul terț de servicii TIC va continua să furnizeze funcțiile sau serviciile respective vizând să reducă riscul de perturbare în cadrul entității financiare;

(b) care permite entității financiare să treacă la un alt furnizor terț de servicii TIC sau să treacă la soluții furnizate la sediu, în conformitate cu complexitatea serviciului furnizat.

3. La negocierea acordurilor contractuale, entitățile financiare și furnizorii terți de servicii TIC țin seama de utilizarea clauzelor contractuale standard, elaborate pentru servicii specifice.

4. AES elaborează, prin intermediul Comitetului comun, proiecte de standarde tehnice de reglementare pentru a aduce precizări suplimentare cu privire la elementele pe care o entitate financiară trebuie să le stabilească și să le evalueze atunci când subcontractează funcții critice sau importante, pentru a pune în aplicare în mod corespunzător dispozițiile alineatului (2) litera (a).

AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la [*JO: a se introduce data - 1 an de la data intrării în vigoare*].

Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la primul paragraf, în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1095/2010 și, respectiv, (UE) nr. 1094/2010.

SECȚIUNEA II

CADRUL DE SUPRAVEGHERE A FURNIZORILOR TERȚI ESENȚIALI DE SERVICII TIC

Articolul 28

Desemnarea furnizorilor terți esențiali de servicii TIC

1. AES, prin intermediul Comitetului comun și la recomandarea Forumului de supraveghere instituit în temeiul articolului 29 alineatul (1):

   (a) desemnează furnizorii terți de servicii TIC care sunt esențiali pentru entitățile financiare, ținând seama de criteriile menționate la alineatul (2);

   (b) desemnează ABE, ESMA sau EIOPA în calitate de supraveghetor principal pentru fiecare furnizor terț esențial de servicii TIC, în funcție de aspectul dacă valoarea totală a activelor entităților financiare care utilizează serviciile furnizorului terț esențial de servicii TIC și care fac obiectul unuia dintre Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 sau (UE) nr. 1095/2010 reprezintă mai mult de jumătate din valoarea activelor totale ale tuturor entităților financiare care utilizează serviciile furnizorului terț esențial de servicii TIC, astfel cum reiese din bilanțurile consolidate sau din bilanțurile individuale, în cazurile în care bilanțurile nu sunt consolidate, ale entităților financiare respective.

2. Desemnarea prevăzută la alineatul (1) litera (a) se bazează pe următoarele criterii:

   (a) impactul sistemic asupra stabilității, continuității sau calității furnizării serviciilor financiare în cazul în care furnizorul terț relevant de servicii TIC s-ar confrunta cu o defecțiune operațională la scară largă în ceea ce privește furnizarea serviciilor sale, ținând seama de numărul de entități financiare cărora furnizorul terț de servicii TIC relevant le oferă servicii;

   (b) caracterul sistemic sau importanța entităților financiare care se bazează pe furnizorul terț de servicii TIC relevant, evaluată în conformitate cu următorii parametri:

      (i) numărul de instituții de importanță sistemică globală (G-SII) sau de alte instituții de importanță sistemică (O-SII) care se bazează pe respectivul furnizor terț de servicii TIC;

(ii) interdependența dintre G-SII sau O-SII menționate la punctul (i) și alte entități financiare, inclusiv situațiile în care G-SII sau O-SII furnizează servicii de infrastructură financiară altor entități financiare;

(c) dependența entităților financiare de serviciile furnizate de furnizorul terț de servicii TIC relevant în ceea ce privește funcțiile critice sau importante ale entităților financiare care implică, în ultimă instanță, același furnizor terț de servicii TIC, indiferent dacă entitățile financiare se bazează direct sau indirect pe aceste servicii, prin intermediul unor acorduri de subcontractare;

(d) gradul de substituibilitate a furnizorului terț de servicii TIC, ținând seama de următorii parametri:

(i) lipsa unor alternative reale, chiar și parțială, având în vedere numărul limitat de furnizori terți de servicii TIC activi pe o anumită piață sau cota de piață deținută de furnizorul terț de servicii TIC relevant sau complexitatea tehnică ori gradul de sofisticare implicat, inclusiv în ceea ce privește orice tehnologie brevetată, sau caracteristicile specifice ale organizației sau activității furnizorului terț de servicii TIC;

(ii) dificultăți în a migra parțial sau integral datele și volumul de lucru relevant de la furnizorul terț de servicii TIC relevant către un alt furnizor, fie ca urmare a costurilor financiare semnificative, a timpului sau a altor tipuri de resurse pe care le poate implica procesul de migrație, fie din cauza unor riscuri TIC sporite sau a altor riscuri operaționale la care poate fi expusă entitatea financiară prin intermediul unei astfel de migrări.

(e) numărul de state membre în care furnizorul terț de servicii TIC relevant oferă servicii;

(f) numărul de state membre în care funcționează entitățile financiare care utilizează furnizorul terț de servicii TIC relevant.

3. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 50, pentru a completa criteriile menționate la alineatul (2).

4. Mecanismul de desemnare menționat la alineatul (1) litera (a) nu se utilizează decât după ce Comisia a adoptat un act delegat în conformitate cu alineatul (3).

5. Mecanismul de desemnare menționat la alineatul (1) litera (a) nu se aplică furnizorilor terți de servicii TIC care fac obiectul unor cadre de supraveghere instituite cu scopul de a sprijini misiunile menționate la articolul 127 alineatul (2) din Tratatul privind funcționarea Uniunii Europene.

6. AES, prin intermediul Comitetului comun, elaborează, publică și actualizează anual lista furnizorilor terți esențiali de servicii TIC la nivelul Uniunii.

7. În sensul alineatului (1) litera (a), autoritățile competente transmit, anual și agregat, Forumului de supraveghere instituit în temeiul articolului 29 rapoartele menționate la articolul 25 alineatul (4). Forumul de supraveghere evaluează dependențele entităților financiare de furnizorii terți de servicii TIC pe baza informațiilor primite de la autoritățile competente.

8. Furnizorii terți de servicii TIC care nu sunt incluși în lista menționată la alineatul (6) pot solicita să fie incluși în lista respectivă.

În sensul primului paragraf, furnizorul terț de servicii TIC transmite o cerere motivată către ABE, ESMA sau EIOPA care, prin intermediul Comitetului comun, decide dacă să includă respectivul furnizor terț de servicii TIC pe această listă, în conformitate cu alineatul (1) litera (a).

Decizia menționată la al doilea paragraf se adoptă și se notifică furnizorului terț de servicii TIC în termen de 6 luni de la primirea cererii.

9. Entitățile financiare nu utilizează un furnizor terț de servicii TIC stabilit într-o țară terță care ar fi desemnat ca fiind esențial în conformitate cu alineatul (1) litera (a) în cazul în care ar fi stabilit în Uniune.

Articolul 29

Structura cadrului de supraveghere

1. Comitetul comun, în conformitate cu articolul 57 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010, instituie Forumul de supraveghere ca subcomitet în scopul sprijinirii activității Comitetului comun și a supraveghetorului principal menționat la articolul 28 alineatul (1) litera (b) în domeniul riscurilor TIC generate de părți terțe în toate sectoarele financiare. Forumul de supraveghere pregătește proiectele de poziții comune și actele comune ale Comitetului comun în acest domeniu.

   Forumul de supraveghere discută periodic evoluțiile relevante cu privire la riscurile și vulnerabilitățile TIC și promovează o abordare consecventă în ceea ce privește monitorizarea riscurilor TIC generate de părți terțe la nivelul Uniunii.

2. Forumul de supraveghere efectuează anual o evaluare colectivă a rezultatelor și a constatărilor activităților de supraveghere desfășurate pentru toți furnizorii terți esențiali de servicii TIC și promovează măsuri de coordonare pentru a spori reziliența operațională digitală a entităților financiare, a încuraja cele mai bune practici în ceea ce privește abordarea riscurilor de concentrare a serviciilor TIC și a studia factorii de diminuare în cazul transferurilor riscurilor la nivel transsectorial.

3. Forumul de supraveghere prezintă criterii de referință cuprinzătoare ale furnizorilor terți esențiali de servicii TIC, care urmează să fie adoptate de Comitetul comun ca poziții comune ale AES, în conformitate cu articolul 56 alineatul (1) din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

4. Forumul de supraveghere este compus din președinții AES și un reprezentant la nivel înalt provenind din personalul actual al autorității competente relevante din fiecare stat membru. Directorii executivi ai fiecărei AES și câte un reprezentant din partea Comisiei Europene, CERS, BCE și ENISA participă la Forumul de supraveghere în calitate de observatori.

5. În conformitate cu articolul 16 din Regulamentul (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010, AES emit orientări privind cooperarea dintre AES și autoritățile competente în sensul prezentei secțiuni, detaliind procedurile și condițiile referitoare la executarea sarcinilor între autoritățile competente și AES, precum și detalii privind schimburile de informații necesare autorităților competente pentru a se asigura că recomandările adresate furnizorilor terți esențiali de servicii TIC de către supraveghetorii principali în conformitate cu articolul 31 alineatul (1) litera (d) sunt urmate.

6. Cerințele prevăzute în prezenta secțiune nu aduc atingere aplicării Directivei (UE) 2016/1148 și a altor norme ale Uniunii privind supravegherea aplicabilă furnizorilor de servicii de cloud computing.

7. AES, prin intermediul Comitetului comun și pe baza lucrărilor pregătitoare desfășurate de Forumul de supraveghere, prezintă anual Parlamentului European, Consiliului și Comisiei un raport privind aplicarea prezentei secțiuni.

Articolul 30

Sarcinile supraveghetorului principal

1. Supraveghetorul principal evaluează dacă fiecare furnizor terț esențial de servicii TIC a instituit norme, proceduri, mecanisme și măsuri cuprinzătoare, solide și eficace de gestionare a riscurilor TIC pe care le poate genera pentru entitățile financiare.

2. Evaluarea prevăzută la alineatul (1) include:

   (a) cerințe privind TIC pentru a asigura, în special, securitatea, disponibilitatea, continuitatea, scalabilitatea și calitatea serviciilor pe care furnizorul terț esențial de servicii TIC le furnizează entităților financiare, precum și capacitatea de a menține în permanență standarde înalte de securitate, confidențialitate și integritate a datelor;

   (b) securitatea fizică care contribuie la asigurarea securității TIC, inclusiv securitatea sediilor, a instalațiilor, a centrelor de date;

   (c) procesele de gestionare a riscurilor, inclusiv politicile de gestionare a riscurilor TIC, planurile de continuitate a activității bazate pe TIC și planul de recuperare a capabilităților TIC în caz de dezastru;

   (d) mecanismele de guvernanță, inclusiv o structură organizatorică cu linii de responsabilitate și norme privind responsabilitatea clare, transparente și coerente, care permit o gestionare eficace a riscurilor TIC;

   (e) identificarea, monitorizarea și raportarea promptă a incidentelor legate de TIC către entitățile financiare, gestionarea și soluționarea acestora, în special a atacurilor cibernetice;

   (f) mecanismele de portabilitate a datelor, de portabilitate și de interoperabilitate a aplicațiilor, care asigură exercitarea efectivă a drepturilor de reziliere de către entitățile financiare;

   (g) testarea sistemelor, a infrastructurii și a controalelor TIC;

   (h) audituri privind TIC;

   (i) utilizarea standardelor naționale și internaționale relevante aplicabile furnizării serviciilor sale TIC către entitățile financiare.

3. Pe baza evaluării menționate la alineatul (1), supraveghetorul principal adoptă un plan de supraveghere individual clar, detaliat și motivat pentru fiecare furnizor terț esențial de servicii TIC. Planul respectiv este comunicat în fiecare an furnizorului terț esențial de servicii TIC.

4. Odată ce s-a convenit cu privire la planurile de supraveghere menționate la alineatul (3) și acestea au fost notificate furnizorilor terți esențiali de servicii TIC, autoritățile competente pot lua măsuri privind furnizorii terți esențiali de servicii TIC numai în acord cu supraveghetorul principal.

Articolul 31

Competențele supraveghetorului principal

1. În scopul îndeplinirii atribuțiilor care îi revin în temeiul prezentei secțiuni, supraveghetorul principal are următoarele competențe:

   (a) de a solicita toate informațiile și documentele relevante în conformitate cu articolul 32;

   (b) de a efectua investigații și inspecții generale în conformitate cu articolele 33 și 34;

   (c) de a solicita rapoarte după încheierea activităților de supraveghere, în care se specifică acțiunile întreprinse sau măsurile de remediere care au fost puse în aplicare de furnizorii terți esențiali de servicii TIC în legătură cu recomandările menționate la litera (d) de la prezentul alineat;

   (d) de a adresa recomandări privind domeniile menționate la articolul 30 alineatul (2), în special privind:

      (i) utilizarea unor cerințe sau procese specifice de securitate și calitate în domeniul TIC, în special în ceea ce privește introducerea de corecții, actualizări, criptări și alte măsuri de securitate pe care supraveghetorul principal le consideră relevante pentru asigurarea securității din perspectiva TIC a serviciilor furnizate entităților financiare;

      (ii) utilizarea termenelor și condițiilor, inclusiv punerea în aplicare tehnică a acestora, în cadrul cărora furnizorii terți esențiali de servicii TIC furnizează servicii entităților financiare, pe care supraveghetorul principal le consideră relevante pentru prevenirea generării unor puncte unice de defecțiune sau a amplificării acestora sau pentru reducerea la minimum a impactului sistemic potențial la nivelul sectorului financiar al Uniunii în cazul unor riscuri de concentrare a serviciilor TIC;

      (iii) în urma examinării, efectuate în conformitate cu articolele 32 și 33, a acordurilor de subcontractare, inclusiv a acordurilor de subcontractare a serviciilor externalizate pe care furnizorii terți esențiali de servicii TIC intenționează să le realizeze cu alți furnizori terți de servicii TIC sau cu subcontractanți de servicii TIC stabiliți într-o țară terță, orice subcontractare planificată, inclusiv subcontractarea serviciilor externalizate, în cazul în care supraveghetorul principal consideră că subcontractarea în continuare poate genera riscuri pentru furnizarea de servicii de către entitatea financiară sau riscuri la adresa stabilității financiare;

      (iv) abținerea de la încheierea unui nou acord de subcontractare, în cazul în care sunt îndeplinite următoarele condiții cumulative:

         – subcontractantul avut în vedere este un furnizor terț de servicii TIC sau un subcontractant de servicii TIC stabilit într-o țară terță;

         – subcontractarea vizează o funcție critică sau importantă a entității financiare.

2. Supraveghetorul principal consultă Forumul de supraveghere înainte de a exercita competențele menționate la alineatul (1).

3. Furnizorii terți esențiali de servicii TIC cooperează cu bună credință cu supraveghetorul principal și îl asistă pe acesta în îndeplinirea sarcinilor sale.

4. Supraveghetorul principal poate impune o penalitate cu titlu cominatoriu pentru a obliga furnizorul terț esențial de servicii TIC să respecte dispozițiile de la alineatul (1) literele (a), (b) și (c).

5. Penalitățile cu titlu cominatoriu menționate la alineatul (4) se impun zilnic până când conformitatea este asigurată și pe o perioadă de maximum șase luni de la data notificării furnizorului terț esențial de servicii TIC.

6. Cuantumul penalității cu titlu cominatoriu, calculat de la data prevăzută în decizia de impunere a penalității cu titlu cominatoriu, este de 1 % din cifra de afaceri zilnică medie globală a furnizorului terț esențial de servicii TIC din exercițiul financiar precedent.

7. Penalitățile sunt de natură administrativă și sunt executorii. Executarea este reglementată de normele de procedură civilă în vigoare în statul membru pe teritoriul căruia au loc inspecțiile și se produce accesul. Plângerile legate de desfășurarea neregulamentară a executării sunt de competența instanțelor judecătorești ale statului membru în cauză. Sumele aferente penalităților se alocă bugetului general al Uniunii Europene.

8. AES face publice toate penalitățile cu titlu cominatoriu aplicate, cu excepția cazurilor în care publicarea lor ar perturba grav piețele financiare sau ar aduce un prejudiciu disproporționat părților implicate.

9. Înainte de a impune o penalitate cu titlu cominatoriu în temeiul alineatului (4), supraveghetorul principal oferă reprezentanților furnizorului terț esențial de servicii TIC care face obiectul procedurilor posibilitatea de a fi audiat cu privire la constatări și își întemeiază deciziile numai pe constatările asupra cărora furnizorul terț esențial de servicii TIC care face obiectul procedurilor a avut ocazia să își prezinte observațiile. Drepturile la apărare ale persoanelor care fac obiectul procedurilor se respectă pe deplin pe durata procedurilor. Aceste persoane au drept de acces la dosar, sub rezerva interesului legitim al altor persoane de a-și proteja secretele de afaceri. Dreptul de acces la dosar nu se extinde și la informațiile confidențiale sau la documentele interne de lucru ale supraveghetorului principal.

Articolul 32

Solicitarea de informații

1. Supraveghetorul principal poate, printr-o simplă cerere sau printr-o decizie, să solicite furnizorilor terți esențiali de servicii TIC să furnizeze toate informațiile necesare pentru ca supraveghetorul principal să își îndeplinească sarcinile în temeiul prezentului regulament, inclusiv toate documentele comerciale sau operaționale relevante, contractele, documentele de politică, rapoartele de audit privind securitatea TIC, rapoartele privind incidentele legate de TIC, precum și orice informații legate de părțile cărora furnizorul terț esențial de servicii TIC le-a externalizat funcții sau activități operaționale.

2. Atunci când trimite o simplă solicitare de informații în temeiul alineatului (1), supraveghetorul principal:

   (a) face trimitere la prezentul articol ca temei juridic al solicitării sale;

   (b) menționează scopul solicitării;

(c) specifică informațiile care sunt solicitate;

(d) stabilește un termen pentru furnizarea informațiilor;

(e) informează reprezentantul furnizorului terț esențial de servicii TIC de la care sunt solicitate informațiile cu privire la faptul că acesta nu este obligat să furnizeze informațiile, dar că, în cazul unui răspuns voluntar la solicitare, informațiile furnizate nu trebuie să fie incorecte sau să inducă în eroare.

3. Atunci când solicită furnizarea de informații în temeiul alineatului (1), supraveghetorul principal:

(a) face trimitere la prezentul articol ca temei juridic al solicitării sale;

(b) menționează scopul solicitării;

(c) specifică informațiile care sunt solicitate;

(d) stabilește un termen pentru furnizarea informațiilor;

(e) indică penalitățile cu titlu cominatoriu prevăzute la articolul 31 alineatul (4) în cazul în care informațiile solicitate sunt furnizate incomplet;

(f) indică dreptul de a contesta decizia în fața comisiei de apel a AES și de a solicita controlul legalității deciziei de către *Curtea de Justiție a Uniunii Europene* („Curtea de Justiție”), în conformitate cu articolele 60 și 61 din Regulamentul (UE) nr. 1093/2010, (UE) nr. 1094/2010 și, respectiv, (UE) nr. 1095/2010.

4. Reprezentanții furnizorilor terți esențiali de servicii TIC furnizează informațiile solicitate. Avocații autorizați în mod corespunzător să acționeze pot furniza informațiile în numele clienților lor. Furnizorii terți esențiali de servicii TIC rămân pe deplin răspunzători în cazul în care informațiile furnizate sunt incomplete, incorecte sau induc în eroare.

5. Supraveghetorul principal trimite, fără întârziere, o copie a deciziei de a furniza informațiile către autoritățile competente ale entităților financiare care folosesc serviciile furnizorilor terți esențiali de servicii TIC.

Articolul 33

Investigații generale

1. Pentru a-și îndeplini sarcinile în temeiul prezentului regulament, supraveghetorul principal, asistat de echipa de examinare menționată la articolul 34 alineatul (1), poate efectua investigațiile necesare cu privire la furnizorii terți de servicii TIC:

2. Supraveghetorul principal este împuternicit:

(a) să examineze evidențele, datele, procedurile și orice alte materiale relevante pentru executarea atribuțiilor sale, indiferent de suportul pe care sunt stocate;

(b) să facă sau să obțină copii certificate ale acestor evidențe, date, proceduri și alte materiale, precum și extrase din acestea;

(c) să convoace reprezentanții furnizorului terț de servicii TIC pentru explicații verbale sau scrise cu privire la fapte sau documente referitoare la obiectul și scopul investigației și să înregistreze răspunsurile;

(d) să intervieveze orice altă persoană fizică sau juridică care consimte să fie intervievată în scopul colectării de informații referitoare la obiectul unei investigații;

(e) să solicite înregistrări ale convorbirilor telefonice și ale traficului de date.

3. Funcționarii și alte persoane autorizate de supraveghetorul principal în scopul efectuării investigației menționate la alineatul (1) își exercită competențele pe baza prezentării unei autorizații scrise în care se specifică obiectul și scopul investigației.

Autorizația respectivă indică, de asemenea, penalitățile cu titlu cominatoriu prevăzute la articolul 31 alineatul (4) aplicabile în cazul în care evidențele, datele, procedurile sau orice alte materiale solicitate sau răspunsurile la întrebările adresate reprezentanților furnizorului terț de servicii TIC nu sunt furnizate sau sunt incomplete.

4. Reprezentanții furnizorilor terți de servicii TIC sunt obligați să se supună investigațiilor pe baza unei decizii a supraveghetorului principal. Decizia specifică obiectul și scopul investigației, penalitățile cu titlu cominatoriu prevăzute la articolul 31 alineatul (4), căile de atac disponibile în temeiul Regulamentelor (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010, precum și dreptul de a solicita controlul legalității deciziei de către Curtea de Justiție.

5. În timp util înainte de investigație, supraveghetorii principali informează autoritățile competente ale entităților financiare care utilizează respectivul furnizor terț de servicii TIC cu privire la investigație și la identitatea persoanelor autorizate.

Articolul 34

Inspecții la fața locului

1. Pentru a-și îndeplini sarcinile în temeiul prezentului regulament, supraveghetorul principal, asistat de echipele de examinare menționate la articolul 35 alineatul (1), poate să introducă și să efectueze toate inspecțiile la fața locului necesare în oricare dintre incintele, terenurile sau proprietățile furnizorilor terți de servicii TIC, cum ar fi sediile sociale, centrele operaționale, sediile secundare, precum și să efectueze inspecții la distanță.

2. Funcționarii și alte persoane autorizate de supraveghetorul principal să efectueze o inspecție la fața locului pot intra în orice astfel de incinte, terenuri sau proprietăți și au toate competențele pentru a sigila orice incinte și orice registre sau evidențe pe perioada inspecției și în măsura în care acest lucru este necesar pentru inspecție.

Aceștia își exercită competențele pe baza prezentării unei autorizații scrise în care se specifică obiectul și scopul inspecției, precum și penalitățile cu titlu cominatoriu prevăzute la articolul 31 alineatul (4), în cazul în care reprezentanții furnizorilor terți de servicii TIC nu se supun inspecției.

3. În timp util înainte de inspecție, supraveghetorii principali informează autoritățile competente ale entităților financiare care utilizează respectivul furnizor terț de servicii TIC.

4. Inspecțiile acoperă întreaga gamă de sisteme TIC, rețele, dispozitive, informații și date relevante care sunt utilizate sau contribuie la furnizarea de servicii către entități financiare.

5. Înainte de orice vizită planificată la fața locului, supraveghetorii principali informează în mod rezonabil furnizorii terți esențiali de servicii TIC, cu excepția cazului în care o astfel de notificare nu este posibilă din cauza unei situații de urgență sau de criză sau în cazul în care aceasta ar conduce la o situație în care inspecția sau auditul nu ar mai fi eficace.

6. Furnizorul terț esențial de servicii TIC se supune inspecțiilor la fața locului dispuse prin decizia supraveghetorului principal. Decizia specifică obiectul și scopul inspecției, stabilește data la care inspecția urmează să înceapă și indică penalitățile cu titlu cominatoriu prevăzute la articolul 31 alineatul (4), căile de atac disponibile în temeiul Regulamentelor (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010, precum și dreptul de a solicita controlul legalității deciziei de către Curtea de Justiție.

7. În cazul în care funcționarii și alte persoane autorizate de supraveghetorul principal consideră că un furnizor terț esențial de servicii TIC se opune unei inspecții dispuse în temeiul prezentului articol, supraveghetorul principal informează furnizorul esențial de servicii TIC cu privire la consecințele unei astfel de opoziții, inclusiv posibilitatea ca autoritățile competente ale entităților financiare relevante să rezilieze acordurile contractuale încheiate cu respectivul furnizor terț esențial de servicii TIC.

Articolul 35

Supravegherea permanentă

1. În desfășurarea investigațiilor generale sau a inspecțiilor la fața locului, supraveghetorii principali sunt asistați de o echipă de examinare, instituită pentru fiecare furnizor terț esențial de servicii TIC.

2. Echipa comună de examinare menționată la alineatul (1) este formată din membri ai personalului supraveghetorului principal și al autorităților competente relevante care supraveghează entitățile financiare cărora furnizorul terț esențial de servicii TIC le oferă servicii, care se vor reuni în scopul pregătirii și executării activităților de supraveghere; echipa comună de examinare este alcătuită din maximum 10 membri. Toți membrii echipei comune de examinare au cunoștințe de specialitate în domeniul riscurilor TIC și operaționale. Echipa comună de examinare lucrează sub coordonarea unui membru al personalului AES desemnat („coordonatorul supraveghetorului principal”).

3. AES, prin intermediul Comitetului comun, elaborează proiecte comune de standarde tehnice de reglementare pentru a aduce precizări suplimentare privind desemnarea membrilor echipei comune de examinare care provin de la autoritățile competente relevante, precum și sarcinile și acordurile de lucru ale echipei de examinare. AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la [*JO: a se introduce data - 1 an de la data intrării în vigoare*].

   Se deleagă Comisiei competența de a adopta standardele tehnice de reglementare menționate la primul paragraf în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și, respectiv, (UE) nr. 1095/2010.

4. În termen de 3 luni de la încheierea unei investigații sau a unei inspecții la fața locului, supraveghetorul principal, după consultarea Forumului de supraveghere, adoptă recomandări care urmează a fi adresate de către supraveghetorul principal furnizorului terț esențial de servicii TIC, în temeiul competențelor menționate la articolul 31.

5. Recomandările menționate la alineatul (4) se comunică imediat furnizorului terț esențial de servicii TIC și autorităților competente ale entităților financiare cărora acesta le furnizează servicii.

În scopul executării activităților de supraveghere, supraveghetorul principal poate lua în considerare certificările relevante ale părții terțe și rapoartele de audit intern sau extern ale furnizorului terț de servicii TIC, puse la dispoziție de furnizorul terț esențial de servicii TIC.

Articolul 36

Armonizarea condițiilor care permit desfășurarea supravegherii

1. AES elaborează, prin intermediul Comitetului comun, proiecte de standarde tehnice de reglementare pentru a preciza:

(a) informațiile care trebuie furnizate de un furnizor terț esențial de servicii TIC în cererea de participare voluntară prevăzută la articolul 28 alineatul (8);

(b) conținutul și formatul rapoartelor care pot fi solicitate în scopul articolului 31 alineatul (1) litera (c);

(c) prezentarea informațiilor, inclusiv a structurii, formatelor și metodelor, pe care un furnizor terț esențial de servicii TIC trebuie să le transmită, să le comunice sau să le raporteze în temeiul articolului 31 alineatul (1);

(d) detaliile evaluării efectuate de autoritățile competente cu privire la măsurile luate de furnizorii terți esențiali de servicii TIC, pe baza recomandărilor supraveghetorilor principali, în conformitate cu articolul 37 alineatul (2).

2. AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 1 ianuarie 20xx [*JO: a se introduce data - 1 an de la data intrării în vigoare*].

Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la primul paragraf, în conformitate cu procedura prevăzută la articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și, respectiv, (UE) nr. 1095/2010.

Articolul 37

Monitorizarea de către autoritățile competente

1. În termen de 30 de zile calendaristice de la primirea recomandărilor emise de supraveghetorii principali, în temeiul articolului 31 alineatul (1) litera (d), furnizorii terți esențiali de servicii TIC informează supraveghetorul principal dacă intenționează să urmeze recomandările respective. Supraveghetorii principali transmit imediat aceste informații autorităților competente.

2. Autoritățile competente desfășoară activități de monitorizare pentru a verifica dacă entitățile financiare iau în considerare riscurile identificate în recomandările adresate furnizorilor terți esențiali de servicii TIC de către supraveghetorul principal, în conformitate cu articolul 31 alineatul (1) litera (d).

3. În conformitate cu articolul 44, autoritățile competente pot solicita entităților financiare să suspende temporar, parțial sau integral, utilizarea sau implementarea

unui serviciu furnizat de furnizorul terț esențial de servicii TIC, până la abordarea riscurilor identificate în recomandările adresate furnizorilor terți esențiali de servicii TIC. În cazul în care este necesar, acestea pot solicita entităților financiare să rezilieze parțial sau integral acordurile contractuale relevante încheiate cu furnizorii terți esențiali de servicii TIC.

4. Atunci când iau deciziile menționate la alineatul (3), autoritățile competente țin seama de tipul și de magnitudinea riscului care nu este abordat de furnizorul terț esențial de servicii TIC, precum și de gravitatea neconformității, având în vedere următoarele criterii:

   (a) gravitatea și durata neconformității;

   (b) dacă neconformitatea a evidențiat deficiențe grave în ceea ce privește procedurile, sistemele de gestionare, gestionarea riscurilor și controalele interne ale furnizorului terț esențial de servicii TIC;

   (c) dacă au fost facilitate sau ocazionate infracțiuni financiare sau dacă acestea au fost imputabile în alt mod neconformității;

   (d) dacă neconformitatea a fost săvârșită în mod intenționat sau din neglijență.

5. Autoritățile competente informează periodic supraveghetorii principali cu privire la abordările și măsurile luate în cadrul atribuțiilor lor de supraveghere în ceea ce privește entitățile financiare, precum și cu privire la măsurile contractuale luate de acestea din urmă, în cazul în care furnizorul terț esențial de servicii TIC nu a aprobat parțial sau în întregime recomandările adresate de supraveghetorul principal.

Articolul 38

Taxele de supraveghere

1. AES percep de la furnizorii terți esențiali de servicii TIC taxe care acoperă integral cheltuielile necesare ale AES în legătură cu îndeplinirea atribuțiilor de supraveghere în temeiul prezentului regulament, inclusiv rambursarea oricăror costuri care ar putea fi suportate ca urmare a activității desfășurate de autoritățile competente care au luat parte la activitățile de supraveghere în conformitate cu articolul 35.

   Cuantumul unei taxe percepute de la un furnizor terț esențial de servicii TIC acoperă toate costurile administrative și este proporțional cu cifra sa de afaceri.

2. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 50 pentru a completa prezentul regulament prin stabilirea valorii taxelor și a modalității de plată a acestora.

Articolul 39

Cooperarea internațională

1. ABE, ESMA și EIOPA pot, în conformitate cu articolul 33 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și, respectiv, (UE) nr. 1095/2010, să încheie acorduri administrative cu autorități de reglementare și de supraveghere din țări terțe pentru a încuraja cooperarea internațională cu privire la riscurile TIC generate de părți terțe în diferite sectoare financiare, în special prin elaborarea de bune practici pentru revizuirea practicilor de gestionare a riscurilor TIC și a controalelor aferente, a măsurilor de atenuare și a răspunsurilor la incidente.

2. AES transmit, prin intermediul Comitetului comun, o dată la cinci ani, un raport confidențial comun Parlamentului European, Consiliului și Comisiei, în care sintetizează constatările discuțiilor relevante purtate cu autoritățile țărilor terțe menționate la alineatul (1), axându-se pe evoluția riscurilor TIC generate de părți terțe și pe implicațiile pentru stabilitatea financiară, integritatea pieței, protecția investitorilor sau funcționarea pieței unice.

CAPITOLUL VI

ACORDURI DE SCHIMB DE INFORMAȚII

Articolul 40

Acorduri de schimb de informații și date operative privind amenințările cibernetice

1. Entitățile financiare pot face schimb reciproc de informații și date operative privind amenințările cibernetice, inclusiv de indicatori de compromitere, tactici, tehnici și proceduri, alerte de securitate cibernetică și instrumente de configurare, în măsura în care aceste schimburi de informații și date operative:

   (a) vizează sporirea rezilienței operaționale digitale a entităților financiare, în special prin sensibilizarea cu privire la amenințările cibernetice, limitarea sau împiedicarea răspândirii amenințărilor cibernetice, sprijinirea gamei de capacități defensive ale entităților financiare, tehnicile de detectare a amenințărilor, strategiile de atenuare sau etapele proceselor de răspuns și de recuperare;

   (b) au loc în cadrul unor comunități de încredere ale entităților financiare;

   (c) sunt puse în aplicare prin intermediul unor acorduri de schimb de informații care protejează natura potențial sensibilă a informațiilor partajate și care sunt reglementate de norme de conduită care respectă pe deplin confidențialitatea comercială, protecția datelor cu caracter personal[48] și orientările privind politica în domeniul concurenței[49].

2. În sensul alineatului (1) litera (c), acordurile de schimb de informații definesc condițiile de participare și, după caz, stabilesc detaliile privind implicarea autorităților publice și calitatea în care acestea din urmă pot fi asociate la acordurile de schimb de informații, precum și elementele operaționale, inclusiv utilizarea platformelor informatice specifice.

3. Entitățile financiare informează autoritățile competente cu privire la participarea lor la acordurile de schimb de informații menționate la alineatul (1), odată cu validarea apartenenței lor sau, după caz, cu încetarea calității de membru, după ce aceasta din urmă intră în vigoare.

---

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

[49] Comunicarea Comisiei – Orientări privind aplicabilitatea articolului 101 din Tratatul privind funcționarea Uniunii Europene acordurilor de cooperare orizontală, 2011/C 11/01.

CAPITOLUL VII

AUTORITĂȚILE COMPETENTE

Articolul 41

Autoritățile competente

Fără a aduce atingere dispozițiilor privind cadrul de supraveghere pentru furnizorii terți esențiali de servicii TIC menționat în capitolul V secțiunea II din prezentul regulament, conformitatea cu obligațiile prevăzute în prezentul regulament este asigurată de următoarele autorități competente în conformitate cu prerogativele conferite prin actele juridice respective:

(a) pentru instituțiile de credit, autoritatea competentă desemnată în conformitate cu articolul 4 din Directiva 2013/36/UE, fără a aduce atingere atribuțiilor specifice conferite BCE prin Regulamentul (UE) nr. 1024/2013;

(b) pentru prestatorii de servicii de plată, autoritatea competentă desemnată în conformitate cu articolul 22 din Directiva (UE) 2015/2366;

(c) pentru instituțiile de plată în monedă electronică, autoritatea competentă desemnată în conformitate cu articolul 37 din Directiva 2009/110/CE;

(d) pentru firmele de investiții, autoritatea competentă desemnată în conformitate cu articolul 4 din Directiva (UE) 2019/2034;

(e) pentru furnizorii de servicii de criptoactive, emitenții de criptoactive, emitenții de tokenuri raportate la active și emitenții de tokenuri semnificative raportate la active, autoritatea competentă desemnată în conformitate cu articolul 3 alineatul (1) litera (ee) prima liniuță din [*Regulamentul (UE) 20xx (Regulamentul MICA)*];

(f) pentru depozitarii centrali de titluri de valoare, autoritatea competentă desemnată în conformitate cu articolul 11 din Regulamentul (UE) nr. 909/2014;

(g) pentru contrapărțile centrale, autoritatea competentă desemnată în conformitate cu articolul 22 din Regulamentul (UE) nr. 648/2012;

(h) pentru locurile de tranzacționare și furnizorii de servicii de raportare a datelor, autoritatea competentă desemnată în conformitate cu articolul 67 din Directiva 2014/65/UE;

(i) pentru registrele centrale de tranzacții, autoritatea competentă desemnată în conformitate cu articolul 55 din Regulamentul (UE) nr. 648/2012;

(j) pentru administratorii de fonduri de investiții alternative, autoritatea competentă desemnată în conformitate cu articolul 44 din Directiva 2011/61/UE;

(k) pentru societățile de administrare, autoritatea competentă desemnată în conformitate cu articolul 97 din Directiva 2009/65/CE;

(l) pentru întreprinderile de asigurare și reasigurare, autoritatea competentă desemnată în conformitate cu articolul 30 din Directiva 2009/138/CE;

(m) pentru intermediarii de asigurări, intermediarii de reasigurări și intermediarii de asigurări auxiliare, autoritatea competentă desemnată în conformitate cu articolul 12 din Directiva (UE) 2016/97;

(n) pentru instituțiile pentru furnizarea de pensii ocupaționale, autoritatea competentă desemnată în conformitate cu articolul 47 din Directiva 2016/2341;

(o) pentru agențiile de rating de credit, autoritatea competentă desemnată în conformitate cu articolul 21 din Regulamentul (CE) nr. 1060/2009;

(p) pentru auditorii statutari și societățile de audit, autoritatea competentă desemnată în conformitate cu articolul 3 alineatul (2) și cu articolul 32 din Directiva 2006/43/CE;

(q) pentru administratorii indicilor de referință critici, autoritatea competentă desemnată în conformitate cu articolele 40 și 41 din *Regulamentul xx/202x*;

(r) pentru furnizorii de servicii de finanțare participativă, autoritatea competentă desemnată în conformitate cu *articolul x din Regulamentul xx/202x*;

(s) pentru registrele centrale de securitizări, autoritatea competentă desemnată în conformitate cu articolul 10 și cu articolul 14 alineatul (1) din Regulamentul (UE) 2017/2402.

Articolul 42

Cooperarea cu structurile și autoritățile înființate prin Directiva (UE) 2016/1148

1. Pentru a încuraja cooperarea și a permite schimburile de informații în scopuri de supraveghere între autoritățile competente desemnate în temeiul prezentului regulament și Grupul de cooperare instituit prin articolul 11 din Directiva (UE) 2016/1148, AES și autoritățile competente pot solicita să fie invitate la lucrările Grupului de cooperare.

2. După caz, autoritățile competente se pot consulta cu punctul unic de contact și cu echipele naționale de intervenție în caz de incidente de securitate informatică, menționate la articolele 8 și 9 din Directiva (UE) 2016/1148.

Articolul 43

Exerciții financiare transsectoriale, comunicare și cooperare

1. AES, prin intermediul Comitetului comun și în colaborare cu autoritățile competente, cu BCE și cu CERS, pot stabili mecanisme care să permită schimbul de practici eficace între sectoarele financiare în vederea îmbunătățirii conștientizării situației și a identificării vulnerabilităților și riscurilor cibernetice comune la nivelul tuturor sectoarelor.

   Acestea pot elabora exerciții de gestionare a crizelor și pentru situații neprevăzute care implică scenarii de atacuri cibernetice, cu scopul de a dezvolta canale de comunicare și de a permite treptat un răspuns coordonat eficace la nivelul UE în cazul unui incident transfrontalier major legat de TIC sau al unei amenințări conexe cu un impact sistemic asupra sectorului financiar al Uniunii în ansamblu.

   Aceste exerciții pot, după caz, să testeze și dependențele sectorului financiar de alte sectoare economice.

2. Autoritățile competente, ABE, ESMA sau EIOPA și BCE cooperează strâns între ele și fac schimb de informații pentru a-și îndeplini atribuțiile în temeiul articolelor 42-48. Acestea își coordonează îndeaproape activitățile de supraveghere, pentru a identifica și a remedia cazurile de nerespectare a prezentului regulament, pentru a elabora și a promova bune practici, a facilita colaborarea, a stimula consecvența interpretării și a furniza evaluări interjurisdicționale în cazul oricăror neînțelegeri.

Articolul 44

Sancțiuni administrative și măsuri de remediere

1. Autoritățile competente dispun de toate competențele de supraveghere, de investigare și de sancționare necesare pentru a-și îndeplini atribuțiile în conformitate cu prezentul regulament.

2. Competențele menționate la alineatul (1) includ cel puțin următoarele:

   (a) competența de a avea acces la orice document sau date deținute sub orice formă pe care autoritatea o consideră relevantă pentru îndeplinirea sarcinilor sale și competența de a primi sau de face o copie a acestora;

   (b) competența de a desfășura inspecții la fața locului sau investigații;

   (c) competența de a solicita măsuri corective și de remediere pentru încălcările cerințelor prezentului regulament.

3. Fără a aduce atingere dreptului statelor membre de a impune sancțiuni penale în conformitate cu articolul 46, statele membre prevăd norme de stabilire a sancțiunilor administrative și a măsurilor de remediere corespunzătoare pentru încălcările prezentului regulament și asigură punerea lor efectivă în aplicare.

   Aceste sancțiuni sau măsuri sunt eficace, proporționale și disuasive.

4. Statele membre conferă autorităților competente competența de a aplica cel puțin următoarele sancțiuni administrative sau măsuri de remediere în cazul încălcării prezentului regulament:

   (a) emiterea unui ordin prin care i se cere persoanei fizice sau juridice să înceteze comportamentul respectiv și să se abțină de la repetarea comportamentului respectiv;

   (b) solicitarea încetării temporare sau permanente a oricărei practici sau oricărui comportament în legătură cu care autoritatea competentă consideră că contravine dispozițiilor prezentului regulament și prevenirea repetării practicii sau a comportamentului în cauză;

   (c) adoptarea oricărui tip de măsură, inclusiv de natură pecuniară, pentru a asigura că entitățile financiare respectă în continuare cerințele legale;

   (d) solicitarea, în măsura în care dreptul intern permite acest lucru, a unor înregistrări existente ale schimburilor de date deținute de un operator de telecomunicații, atunci când există o suspiciune rezonabilă privind o încălcare a prezentului regulament și atunci când aceste înregistrări pot fi relevante pentru o investigație referitoare la încălcări ale prezentului regulament; și

   (e) emiterea unor anunțuri publice, inclusiv a unor declarații publice care indică identitatea persoanei fizice sau juridice și natura încălcării.

5. Atunci când dispozițiile menționate la alineatul (2) litera (c) și la alineatul (4) se aplică unor persoane juridice, statele membre conferă autorităților competente competența de a aplica sancțiunile administrative și măsurile corective, sub rezerva condițiilor prevăzute în dreptul intern, membrilor organului de conducere, precum și altor persoane care, în temeiul dreptului intern, sunt responsabile de încălcare.

6. Statele membre se asigură că orice decizie de impunere a unor sancțiuni administrative sau a unor măsuri de remediere prevăzute la alineatul (2) litera (c) este justificată în mod corespunzător și face obiectul unei căi de atac.

Articolul 45

Exercitarea competenței de a impune sancțiuni administrative și măsuri de remediere

1. Autoritățile competente își exercită competențele de a impune sancțiunile administrative și măsurile de remediere menționate la articolul 44 în conformitate cu cadrele lor juridice naționale, după caz:

   (a) în mod direct;

   (b) în colaborare cu alte autorități;

   (c) sub propria lor responsabilitate, prin delegare către alte autorități;

   (d) prin sesizarea autorităților judiciare competente.

2. La stabilirea tipului și a nivelului unei sancțiuni administrative sau al unei măsuri de remediere impuse în temeiul articolului 44, autoritățile competente iau în considerare măsura în care încălcarea este intenționată sau rezultă din neglijență și toate celelalte circumstanțe relevante, inclusiv, după caz:

   (a) importanța, gravitatea și durata încălcării;

   (b) gradul de responsabilitate al persoanei fizice sau juridice responsabile de încălcare;

   (c) puterea financiară a persoanei fizice sau juridice responsabile;

   (d) importanța profiturilor obținute sau a pierderilor evitate de către persoana fizică sau juridică responsabilă, în măsura în care acestea pot fi determinate;

   (e) pierderile suferite de părți terțe în urma respectivei încălcări, în măsura în care acestea pot fi determinate;

   (f) nivelul de cooperare cu autoritatea competentă a persoanei fizice sau juridice responsabile, fără a aduce atingere necesității de a asigura confiscarea profiturilor obținute sau a pierderilor evitate de persoana respectivă;

   (g) încălcările anterioare comise de persoana fizică sau juridică responsabilă.

Articolul 46

Sancțiuni penale

1. Statele membre pot decide să nu stabilească norme privind sancțiunile administrative sau măsurile de remediere în cazul încălcărilor care fac obiectul sancțiunilor penale în dreptul lor intern.

2. În cazul în care statele membre au ales să prevadă sancțiuni penale pentru încălcările prezentului regulament, acestea se asigură că sunt instituite măsuri adecvate astfel

încât autoritățile competente să dispună de toate competențele necesare pentru a asigura legătura cu autoritățile judiciare, de urmărire penală sau de justiție penală din jurisdicția lor pentru a primi informații specifice referitoare la anchete sau proceduri penale inițiate pentru încălcarea prezentului regulament, precum și pentru a furniza aceleași informații altor autorități competente, precum și ABE, ESMA sau EIOPA astfel încât să își îndeplinească obligațiile de cooperare în scopul prezentului regulament.

Articolul 47

Obligații de notificare

Statele membre notifică actele cu putere de lege și actele administrative care pun în aplicare prezentul capitol, inclusiv orice dispoziții relevante de drept penal, Comisiei, ESMA, ABE și EIOPA până la [*JO: a se introduce data - 1 an de la data intrării în vigoare*]. Statele membre notifică fără întârzieri nejustificate Comisiei, ESMA, ABE și EIOPA orice modificare ulterioară a acestor acte.

Articolul 48

Publicarea sancțiunilor administrative

1. Autoritățile competente publică pe site-urile lor internet oficiale, fără întârzieri nejustificate, orice decizie de impunere a unei sancțiuni administrative care nu este atacată după notificarea destinatarului sancțiunii cu privire la decizia respectivă.

2. Publicarea menționată la alineatul (1) include informații privind tipul și natura încălcării, identitatea persoanelor responsabile și sancțiunile impuse.

3. În cazul în care autoritatea competentă, în urma unei evaluări de la caz la caz, consideră că publicarea identității, în cazul persoanelor juridice, sau a identității și a datelor cu caracter personal, în cazul persoanelor fizice, ar fi disproporționată, ar pune în pericol stabilitatea piețelor financiare sau desfășurarea unei anchete penale în curs sau ar cauza, în măsura în care acestea pot fi determinate, daune disproporționate persoanei implicate, aceasta adoptă una dintre următoarele soluții în ceea ce privește decizia de impunere a unei sancțiuni administrative:

   (a) amână publicarea sa până în momentul în care toate motivele pentru nepublicare încetează;

   (b) publică decizia în mod anonim, în conformitate cu legislația națională; sau

   (c) se abține de la publicarea acesteia, în cazul în care opțiunile prevăzute la literele (a) și (b) sunt considerate insuficiente pentru a garanta lipsa oricărui pericol pentru stabilitatea piețelor financiare sau în cazul în care o astfel de publicare nu ar fi proporțională cu indulgența sancțiunii impuse.

4. În cazul unei decizii de a publica sancțiunea administrativă cu titlu anonim în conformitate cu alineatul (3) litera (b), publicarea datelor relevante poate fi amânată.

5. Dacă o autoritate competentă publică o decizie de impunere a unei sancțiuni administrative care face obiectul unei căi de atac în fața autorităților judiciare relevante, autoritățile competente includ imediat pe site-ul lor internet oficial această informație și, ulterior, orice informații conexe ulterioare cu privire la rezultatul căii de atac. Se publică, de asemenea, hotărârile judecătorești care anulează deciziile de impunere a unei sancțiuni administrative.

6. Autoritățile competente se asigură că orice publicare menționată la alineatele (1)-(4) rămâne pe site-ul lor internet oficial timp de cel puțin cinci ani de la publicare. Datele cu caracter personal conținute în publicare se păstrează pe site-ul internet oficial al autorității competente numai pe perioada necesară în conformitate cu normele aplicabile privind protecția datelor.

Articolul 49

Secretul profesional

1. Informațiile confidențiale primite, schimbate sau transmise în temeiul prezentului regulament fac obiectul condițiilor privind respectarea secretului profesional prevăzute la alineatul (2).
2. Obligația de păstrare a secretului profesional se aplică tuturor persoanelor care lucrează sau care au lucrat pentru autoritățile competente în temeiul prezentului regulament sau pentru orice autoritate, întreprindere de pe piață sau persoană fizică ori juridică căreia autoritatea competentă i-a delegat competențe ale sale, inclusiv auditorii și experții contractați de autoritatea competentă.
3. Informațiile care fac obiectul obligației de păstrare a secretului profesional nu pot fi comunicate niciunei alte persoane sau autorități, exceptând cazurile în care se invocă temeiul dispozițiilor dreptului Uniunii sau ale dreptului național.
4. Toate informațiile care fac obiectul unor schimburi între autoritățile competente în conformitate cu prezentul regulament și care privesc condițiile comerciale sau operaționale și alte chestiuni economice sau personale sunt considerate confidențiale și intră sub incidența obligației secretului profesional, cu excepția cazului în care autoritatea competentă precizează, la momentul comunicării, că informațiile respective pot fi divulgate sau a cazului în care divulgarea acestora este necesară pentru proceduri judiciare.

CAPITOLUL VIII

ACTE DELEGATE

Articolul 50

Exercitarea delegării de competențe

1. Se conferă Comisiei competența de a adopta acte delegate, cu respectarea condițiilor stabilite la prezentul articol.
2. Competența de a adopta acte delegate menționată la articolul 28 alineatul (3) și la articolul 38 alineatul (2) se conferă Comisiei pentru o perioadă de cinci ani de la [OP: vă rugăm introduceți data - 5 ani de la data intrării în vigoare a prezentului regulament].
3. Delegarea de competențe menționată la articolul 28 alineatul (3) și la articolul 38 alineatul (2) poate fi revocată în orice moment de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării competenței specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării

acesteia în *Jurnalul Oficial al Uniunii Europene* sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.

4. Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare.

5. Imediat ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

6. Un act delegat adoptat în temeiul articolului 28 alineatul (3) și al articolului 38 alineatul (2) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Termenul respectiv se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

CAPITOLUL IX

DISPOZIȚII TRANZITORII ȘI FINALE

SECȚIUNEA I

Articolul 51

Clauza de reexaminare

Până la [*OP: a se introduce data: 5 ani de la data intrării în vigoare a prezentului regulament*], după ce se consultă cu ABE, ESMA, EIOPA și CERS, după caz, Comisia efectuează o revizuire și prezintă un raport Parlamentului European și Consiliului, însoțit, dacă este cazul, de o propunere legislativă, privind criteriile de desemnare a furnizorilor terți esențiali de servicii TIC menționate la articolul 28 alineatul (2).

SECȚIUNEA II

MODIFICĂRI

Articolul 52

Modificări aduse Regulamentului (CE) nr. 1060/2009

În anexa I la Regulamentul (CE) nr. 1060/2009, secțiunea A punctul 4 primul paragraf se înlocuiește cu următorul text:

„Agenția de rating de credit dispune de proceduri contabile și administrative sigure, de mecanisme de control intern, de tehnici eficiente de evaluare a riscurilor și de dispozitive eficiente de control și de salvgardare pentru gestionarea sistemelor TIC în conformitate cu Regulamentul (UE) 2021/xx al Parlamentului European și al Consiliului * [DORA].

* Regulamentul (UE) 2021/xx al Parlamentului European și al Consiliului […] (JO L XX, ZZ.LL.AAAA, p. X).”.

Articolul 53

Modificări aduse Regulamentului (UE) nr. 648/2012

Regulamentul (UE) nr. 648/2012 se modifică după cum urmează:

(1) Articolul 26 se modifică după cum urmează:

(a) alineatul (3) se înlocuiește cu următorul text:

„(3) CPC mențin și utilizează o structură organizatorică adecvată pentru a le asigura continuitatea și funcționarea corespunzătoare în cursul prestării serviciilor și al desfășurării activităților. Ele utilizează sisteme, resurse și proceduri adecvate și proporționale, inclusiv sisteme TIC gestionate în conformitate cu Regulamentul (UE) 2021/xx al Parlamentului European și al Consiliului * [DORA].

* Regulamentul (UE) 2021/xx al Parlamentului European și al Consiliului […](JO L XX, ZZ.LL.AAAA, p. X).”;

(b) alineatul (6) se elimină;

(2) Articolul 34 se modifică după cum urmează:

(a) alineatul (1) se înlocuiește cu următorul text:

„(1) CPC prevăd, aplică și mențin o politică adecvată de continuitate a activității și un plan de recuperare în caz de dezastru, care includ planul de continuitate a activității bazate pe TIC și planul de recuperare a capabilităților TIC în caz de dezastru, instituite în conformitate cu Regulamentul (UE) 2021/xx [DORA], cu scopul de a asigura conservarea funcțiilor lor, reluarea rapidă a operațiunilor și îndeplinirea obligațiilor.”;

(b) la alineatul (3), primul paragraf se înlocuiește cu următorul text:

„Pentru a asigura aplicarea consecventă a prezentului articol, ESMA, după consultarea membrilor SEBC, elaborează proiecte de standarde tehnice de reglementare în care precizează conținutul și cerințele minime ale politicii de continuitate a activității și ale planului de recuperare în caz de dezastru, excluzând planul de continuitate a activității bazate pe TIC și planul de recuperare a capabilităților TIC în caz de dezastru.”;

(3) La articolul 56, alineatul (3) primul paragraf se înlocuiește cu următorul text:

„(3) Pentru a asigura aplicarea consecventă a prezentului articol, ESMA elaborează proiecte de standarde tehnice de reglementare în care precizează detaliile, altele decât cele pentru cerințele legate de gestionarea riscurilor TIC, ale cererii de înregistrare menționate la alineatul (1).”;

(4) la articolul 79, alineatele (1) și (2) se înlocuiesc cu următorul text:

„(1) Registrele centrale de tranzacții identifică sursele de risc operațional și le reduc la minimum prin dezvoltarea unor sisteme, mijloace de control și proceduri adecvate, inclusiv sisteme TIC gestionate în conformitate cu Regulamentul (UE) 2021/xx *[DORA*].

(2) Registrele centrale de tranzacții prevăd, aplică și mențin o politică adecvată de continuitate a activității și un plan de recuperare în caz de dezastru, inclusiv planul de continuitate a activității bazate pe TIC și planul de recuperare a capabilităților TIC în caz de dezastru instituite în conformitate cu Regulamentul (UE) 2021/xx*[DORA],* cu scopul de a asigura menținerea funcțiilor lor, reluarea rapidă a operațiunilor și îndeplinirea obligațiilor.";

(5) la articolul 80, se elimină alineatul (1).

Articolul 54

Modificări aduse Regulamentului (UE) nr. 909/2014

Articolul 45 din Regulamentul (UE) nr. 909/2014 se modifică după cum urmează:

(1) alineatul (1) se înlocuiește cu următorul text:

„(1) CSD-urile identifică sursele de riscuri operaționale, atât interne, cât și externe, și reduc la minimum impactul acestora și prin implementarea unor instrumente, procese și politici TIC adecvate, instituite și gestionate în conformitate cu Regulamentul (UE) 2021/xx al Parlamentului European și al Consiliului*[*DORA*], precum și prin orice alte instrumente, mecanisme de control și proceduri adecvate relevante pentru alte tipuri de risc operațional, inclusiv pentru toate sistemele de decontare a titlurilor de valoare pe care le exploatează.

* Regulamentul (UE) 2021/xx al Parlamentului European și al Consiliului […](JO L XX, ZZ.LL.AAAA, p. X).";

(2) alineatul (2) se elimină;

(3) alineatele (3) și (4) se înlocuiesc cu următorul text:

„(3) Pentru serviciile pe care le prestează, precum și pentru fiecare sistem de decontare a titlurilor de valoare pe care îl exploatează, CSD-urile prevăd, aplică și mențin un plan adecvat de asigurare a continuității activității și de recuperare în caz de dezastru, inclusiv planul privind continuitatea activității bazate pe TIC și planul de recuperare a capabilităților TIC în caz de dezastru instituite în conformitate cu Regulamentul (UE) 2021/xx[DORA], cu scopul de a asigura continuitatea serviciilor lor, reluarea rapidă a operațiunilor și îndeplinirea obligațiilor CSD-urilor în cazul unor evenimente care prezintă un risc semnificativ de perturbare a operațiunilor.

(4) Planul menționat la alineatul (3) prevede reluarea tuturor tranzacțiilor și pozițiilor participanților în momentul perturbării, pentru a permite participanților la un CSD să continue să funcționeze în condiții de siguranță și să efectueze decontarea la data stabilită, inclusiv prin garantarea faptului că sistemele IT esențiale pot relua operațiunile aflate în curs în momentul perturbării, astfel cum se prevede la articolul 11 alineatele (5) și (7) din Regulamentul (UE) 2021/xx [DORA].";

(4) la alineatul (6), primul paragraf se înlocuiește cu următorul text*:*

„CSD-urile identifică, monitorizează și gestionează riscurile pe care le pot prezenta pentru operațiunile lor participanții principali la sistemele de decontare a titlurilor de valoare pe care le exploatează, precum și furnizorii de servicii și utilități, dar și alte CSD-uri sau alte infrastructuri ale piețelor. La cerere, CSD-urile furnizează autorităților competente și relevante informații cu privire la orice astfel de riscuri

identificate. De asemenea, acestea informează autoritatea competentă și autoritățile relevante, fără întârziere, cu privire la orice incident operațional, altul decât cele legate de riscurile TIC, care rezultă din astfel de riscuri.”;

(5) la alineatul (7), primul paragraf se înlocuiește cu următorul text*:*

„ESMA elaborează, în strânsă cooperare cu membrii SEBC, proiecte de standarde tehnice de reglementare care să precizeze riscurile operaționale menționate la alineatele (1) și (6), altele decât riscurile TIC, metodele de testare, abordare și reducere la minimum a riscurilor respective, inclusiv politicile de asigurare a continuității activității și planurile de recuperare în caz de dezastru menționate la alineatele (3) și (4), precum și modalitățile de evaluare a acestora.”.

Articolul 55

Modificări aduse Regulamentului (UE) nr. 600/2014

Regulamentul (UE) nr. 600/2014 se modifică după cum urmează:

(1) Articolul 27g se modifică după cum urmează:

(a) alineatul (4) se elimină;

(b) la alineatul (8), litera (c) se înlocuiește cu următorul text:

(c) „(c) cerințele organizatorice concrete prevăzute la alineatele (3) și (5).”;

(2) Articolul 27h se modifică după cum urmează:

(a) alineatul (5) se elimină;

(b) la alineatul (8), litera (e) se înlocuiește cu următorul text:

„(e) cerințele organizatorice concrete prevăzute la alineatul (4).”;

(3) Articolul 27i se modifică după cum urmează:

(a) alineatul (3) se elimină;

(b) la alineatul (5), litera (b) se înlocuiește cu următorul text:

„(b) cerințele organizatorice concrete prevăzute la alineatele (2) și (4).”.

Articolul 56

Intrarea în vigoare și aplicarea

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării sale în *Jurnalul Oficial al Uniunii Europene*.

Se aplică de la [*OP: a se introduce data – 12 luni de la data intrării în vigoare*].

Totuși, articolele 23 și 24 se aplică de la [*OP: a se introduce data – 36 de luni de la data intrării în vigoare a prezentului regulament*].

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. Denumirea propunerii/inițiativei

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

1.3. Caracterul propunerii/inițiativei

1.4. Obiectiv(e)

1.5. Motivele propunerii/inițiativei

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

2.3. 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 estimat asupra cheltuielilor

3.2.1. Sinteza impactului estimat asupra cheltuielilor

3.2.2. Impactul estimat asupra creditelor

3.2.3. Impactul estimat asupra resurselor umane

3.2.4. Compatibilitatea cu actualul cadru financiar multianual

3.2.5. Contribuțiile terților

3.3. Impactul estimat asupra veniturilor

Anexă

Ipoteze generale

Competențe de supraveghere

FIȘĂ FINANCIARĂ LEGISLATIVĂ „AGENȚII”

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Denumirea propunerii/inițiativei

Propunere de regulament al Parlamentului European și al Consiliului privind reziliența operațională digitală a sectorului financiar.

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

Domeniul de politică: Stabilitate financiară, servicii financiare și uniunea piețelor de capital

Activitatea: Reziliența operațională digitală

1.3. Propunerea/inițiativa se referă la

☑ **o acțiune nouă**

☐ **o acțiune nouă ca urmare a unui proiect-pilot/a unei acțiuni pregătitoare**[50]

☐ **prelungirea unei acțiuni existente**

☐ **o fuziune a uneia sau mai multor acțiuni către o altă/o nouă acțiune**

1.4. Obiectiv(e)

1.4.1. Obiectiv(e) general(e)

Obiectivul general al inițiativei este acela de a consolida reziliența operațională digitală a entităților din sectorul financiar din UE prin simplificarea și modernizarea normelor existente și prin introducerea unor noi cerințe acolo unde există lacune. Aceasta ar consolida, de asemenea, cadrul unic de reglementare în ceea ce privește dimensiunea sa digitală.

Obiectivul global poate fi structurat în trei obiective generale: (1) reducerea riscului de perturbare și instabilitate financiară, (2) reducerea sarcinii administrative și creșterea eficacității supravegherii, și (3) sporirea protecției consumatorilor și a investitorilor.

1.4.2. Obiectiv(e) specific(e)

Propunerea are următoarele obiective specifice:

Abordarea riscurilor legate de tehnologiile informației și comunicațiilor (TIC) într-un mod mai cuprinzător și consolidarea nivelului general de reziliență digitală a sectorului financiar;

Simplificarea raportării incidentelor legate de TIC și abordarea cerințelor de raportare care se suprapun;

Asigurarea accesului autorităților de supraveghere financiară la informații privind incidentele legate de TIC;

Asigurarea evaluării, de către entitățile financiare care fac obiectul prezentei propuneri, a eficacității măsurilor lor preventive și de reziliență, precum și a identificării vulnerabilitățile legate de TIC;

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

Reducerea fragmentării pieței unice și asigurarea acceptării la nivel transfrontalier a rezultatelor testelor. Consolidarea garanțiilor contractuale pentru entitățile financiare atunci când utilizează servicii TIC, inclusiv pentru normele privind externalizarea (care reglementează monitorizarea furnizorilor terți de servicii TIC); Permiterea supravegherii activităților furnizorilor terți esențiali de servicii TIC; Stimularea schimbului de date operative privind amenințările în sectorul financiar.

1.4.3. Rezultatul (rezultatele) și impactul preconizate

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

Un act privind reziliența operațională digitală a sectorului financiar ar asigura un cadru cuprinzător care acoperă toate aspectele rezilienței operaționale digitale și ar fi eficace în îmbunătățirea rezilienței operaționale globale a sectorului financiar. Acesta ar garanta claritatea și coerența la nivelul cadrului unic de reglementare.

De asemenea, actul ar spori claritatea și coerența interacțiunii cu Directiva NIS și cu versiunea revizuită a acesteia. Acesta ar aduce clarificări entităților financiare cu privire la diferitele norme privind reziliența operațională digitală pe care acestea trebuie să le respecte, în special în cazul entităților financiare care dețin mai multe autorizații și își desfășoară activitatea pe diferite piețe din UE.

1.4.4. Indicatori de performanță

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

Indicatori posibili:

Numărul de incidente legate de TIC în sectorul financiar al UE și impactul acestora

Numărul de incidente majore legate de TIC care au fost raportate autorităților de supraveghere prudențială

Numărul de entități financiare care ar fi obligate să efectueze teste de penetrare bazate pe amenințări (*threat-led penetration tests* – TLPT)

Numărul de entități financiare care utilizează clauzele contractuale standard pentru a încheia acorduri contractuale cu furnizori terți de servicii TIC

Numărul de furnizori terți esențiali de servicii TIC supravegheați de AES/autoritățile de supraveghere prudențială

Numărul de entități financiare care participă la soluții de partajare de date operative privind amenințările

Numărul de autorități care trebuie să primească rapoarte cu privire la același incident legat de TIC

Numărul de teste TLPT transfrontaliere

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

Sectorul financiar se bazează în mare măsură pe tehnologiile informației și comunicațiilor (TIC). În pofida progreselor semnificative realizate prin inițiative politice și legislative țintite de la nivel național și european, riscurile TIC reprezintă în continuare o provocare pentru reziliența operațională, performanța și stabilitatea sistemului financiar al UE. Reforma care a urmat crizei financiare din 2008 a consolidat în primul rând reziliența financiară a sectorului financiar al UE și a vizat protejarea competitivității și a stabilității UE din punct de vedere economic, prudențial și al comportamentului pe piață. Securitatea TIC și reziliența operațională digitală globală fac parte din riscul operațional, dar au fost mai puțin evidente pe agenda de reglementare post-criză, dezvoltându-se doar în unele domenii ale politicii și

reglementării privind pieţele financiare din UE sau numai în câteva state membre. Acest lucru se materializează în următoarele provocări, pe care propunerea ar trebui să le abordeze:

Cadrul juridic al UE care acoperă riscurile TIC şi reziliența operațională la nivelul sectorului financiar este fragmentat şi nu este pe deplin consecvent.

Lipsa unor cerinţe coerente de raportare a incidentelor legate de TIC conduce la o imagine de ansamblu incompletă pe care autorităţile de supraveghere o au cu privire la natura, frecvenţa, semnificaţia şi impactul incidentelor.

Unele entităţi financiare se confruntă cu cerinţe de raportare complexe, care se suprapun şi sunt potenţial inconsecvente cu privire la acelaşi incident legat de TIC.

Schimbul insuficient de informaţii şi cooperarea insuficientă cu privire la datele operative referitoare la ameninţările cibernetice la nivel strategic, tactic şi operaţional împiedică entităţile financiare să evalueze şi să monitorizeze în mod adecvat ameninţările cibernetice, precum şi să asigure protecţie şi să răspundă în mod corespunzător în cazul unor astfel de ameninţări.

În anumite subsectoare financiare, pot exista cadre multiple şi necoordonate pentru testele de penetrare şi testele privind reziliența, cuplate cu o lipsă a unei recunoaşteri transfrontaliere a rezultatelor, în timp ce alte subsectoare nu dispun de astfel de cadre de testare.

Lipsa de informaţii în materie de supraveghere cu privire la activităţile entităţilor financiare care primesc servicii de la furnizori terţi de servicii TIC expune entităţile financiare, în mod individual, şi întregul sistem financiar la riscuri operaţionale.

Autorităţile de supraveghere financiară nu dispun de un mandat suficient şi nici de instrumente de monitorizare şi de gestionare a riscurilor de concentrare şi a celor sistemice generate de dependenţa entităţilor financiare de furnizori terţi de servicii TIC.

1.5.2. Valoarea adăugată a intervenţiei Uniunii (aceasta poate rezulta din diferiţi factori, de exemplu o mai bună coordonare, securitatea juridică, o eficacitate sporită sau complementarităţi multiple). În scopul prezentului punct, „valoarea adăugată a intervenţiei Uniunii” reprezintă valoarea rezultată din intervenţia Uniunii care depăşeşte valoarea care ar fi fost altfel creată prin simpla intervenţie a statelor membre.

Motivele acţiunii la nivel european (ex ante):

Reziliența operațională digitală este o chestiune de interes comun pentru pieţele financiare ale UE. Acţiunea la nivelul UE ar aduce mai multe avantaje şi o valoare mai mare decât acţiunile întreprinse separat la nivel naţional. Fără a adăuga aceste dispoziţii operaţionale privind riscurile TIC, cadrul unic de reglementare ar oferi instrumentele necesare pentru a aborda toate celelalte tipuri de riscuri la nivel european, dar ar exclude aspectele legate de reziliența operațională digitală sau le-ar include în iniţiative fragmentate şi necoordonate la nivel naţional. Propunerea ar oferi claritate juridică cu privire la oportunitatea şi modul în care se aplică dispoziţiile operaţionale digitale, în special în cazul entităţilor financiare transfrontaliere, şi ar elimina necesitatea ca statele membre să îşi îmbunătăţească în mod individual normele, standardele şi aşteptările în ceea ce priveşte reziliența operațională şi securitatea cibernetică, ca răspuns la actuala acoperire limitată asigurată de normele UE şi la caracterul general al Directivei NIS.

Valoarea adăugată pe care se preconizează că o va avea intervenţia Uniuni (ex post):

Intervenția Uniunii ar spori în mod semnificativ eficacitatea politicii, reducând în același timp complexitatea și diminuând sarcina financiară și administrativă pentru toate entitățile financiare. Aceasta ar armoniza un domeniu al economiei care este atât de profund interconectat și integrat și care beneficiază deja de un set unic de norme și de supraveghere. În ceea ce privește raportarea incidentelor legate de TIC, propunerea ar reduce sarcina de raportare – și costurile implicite – în cazul raportării aceluiași incident legat de TIC către autorități diferite din UE și/sau naționale. Aceasta va facilita, de asemenea, recunoașterea/acceptarea reciprocă a rezultatelor testelor entităților care operează la nivel transfrontalier și care fac obiectul mai multor cadre de testare din diferite state membre.

1.5.3. Învățăminte desprinse din experiențele anterioare similare

Inițiativă nouă

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

Obiectivul prezentei propuneri este în concordanță cu o serie de alte politici și inițiative în curs ale UE, în special Directiva privind securitatea rețelelor și a sistemelor informatice (NIS) și Directiva privind infrastructura critică europeană (ICE). Propunerea ar menține beneficiile asociate cadrului orizontal privind securitatea cibernetică prin menținerea celor trei subsectoare financiare în domeniul de aplicare al Directivei NIS. Prin menținerea asocierii cu ecosistemul NIS, autoritățile de supraveghere financiară ar fi în măsură să facă schimb de informații relevante cu autoritățile din domeniul NIS și să participe la Grupul de cooperare NIS. Propunerea nu ar avea un impact asupra Directivei NIS, ci s-ar baza mai degrabă pe aceasta și ar aborda posibilele suprapuneri printr-o derogare sub forma unei *lex specialis*. Interacțiunea dintre regulamentul privind serviciile financiare și Directiva NIS ar continua să fie reglementată de o clauză *lex specialis*, excluzând astfel entitățile financiare de la cerințele de fond din Directiva NIS și evitând suprapunerile dintre cele două acte. În plus, propunerea este în concordanță cu Directiva privind infrastructura critică europeană (ICE), aflată în prezent în curs de revizuire pentru a spori protecția și reziliența infrastructurii critice împotriva amenințărilor care nu sunt de natură cibernetică.

Această propunere nu ar avea un impact asupra cadrului financiar multianual (CFM). În primul rând, cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC va fi finanțat în întregime din taxele percepute de la acești furnizori; în al doilea rând, sarcinile de reglementare suplimentare legate de reziliența operațională digitală încredințate AES vor fi asigurate prin redistribuirea internă a personalului existent.

Acest lucru se va traduce printr-o propunere de suplimentare a personalului autorizat al agenției în cadrul viitoarei proceduri bugetare anuale. Agenția va continua să depună eforturi în vederea maximizării sinergiilor și a creșterii eficienței (printre altele, prin intermediul sistemelor informatice) și va monitoriza îndeaproape volumul de muncă suplimentar aferent prezentei propuneri, care ar urma să fie reflectat de nivelul personalului autorizat solicitat de agenție în cadrul procedurii bugetare anuale.

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

Au fost luate în considerare mai multe opțiuni de finanțare:

În primul rând, costurile suplimentare ar putea fi finanțate prin mecanismul de finanțare obișnuit al AES. Acest lucru ar implica totuși o creștere substanțială a contribuției UE la resursele financiare ale AES.

Această opțiune este aleasă pentru costurile legate de sarcinile de reglementare corelate cu prezenta propunere. Într-adevăr, AES li se va cere să redistribuie personalul existent pentru a elabora o serie de standarde tehnice. Cu toate acestea, costurile suplimentare legate de supravegherea furnizorilor terți esențiali nu ar putea fi acoperite printr-o redistribuire a resurselor în cadrul AES, care au și alte sarcini pe lângă cele prevăzute în prezenta propunere, precum și în alte acte legislative ale Uniunii. Totodată, sarcinile de supraveghere legate de reziliența operațională digitală necesită expertiză și cunoștințe tehnice specifice. Întrucât nivelul actual al acestor resurse în cadrul AES este insuficient, sunt necesare resurse suplimentare.

În cele din urmă, potrivit propunerii, taxele vor fi percepute de la furnizorii terți esențiali de servicii TIC care fac obiectul supravegherii. Acestea sunt menite să acopere toate resursele suplimentare necesare AES pentru a-și îndeplini noile sarcini și competențe.

1.6. Durata și impactul financiar ale propunerii/inițiativei

☐ **durată limitată**

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

☐ Impactul financiar din AAAA până în AAAA

☑ **durată nedeterminată**

Punere în aplicare cu o perioadă de creștere în intensitate din 2021

urmată de o perioadă de funcționare la capacitate maximă.

1.7. Modul (modurile) de gestiune preconizat(e)[51]

Gestiune directă asigurată de Comisie

☐ prin intermediul agențiilor executive

☐ **Gestiune partajată** cu statele membre

☑ **Gestiune indirectă**, cu delegarea sarcinilor de execuție bugetară:

☐ organizațiilor internaționale și agențiilor acestora (a se preciza);

☐BEI și Fondului european de investiții;

☑ organismelor menționate la articolele 70 și 71;

☐ organismelor de drept public;

☐ organismelor de drept privat cu misiune de serviciu public, cu condiția să prezinte garanții financiare adecvate;

☐ 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;

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

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

Observații

N/A

2. MĂSURI DE GESTIUNE

2.1. Dispoziții în materie de monitorizare și de raportare

A se preciza frecvența și condițiile aferente monitorizării și raportării.

În conformitate cu dispozițiile deja existente, AES elaborează rapoarte periodice privind activitatea lor (inclusiv rapoarte interne către conducerea de nivel superior, rapoarte către consiliile de administrație și raportul anual) și fac obiectul auditurilor efectuate de Curtea de Conturi și de Serviciul de Audit Intern al Comisiei cu privire la utilizarea resurselor și la performanță. Monitorizarea și raportarea acțiunilor incluse în propunere vor respecta cerințele deja existente, precum și noile cerințe care decurg din prezenta propunere.

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

Gestionarea va fi indirectă prin intermediul AES. Mecanismul de finanțare va fi pus în aplicare prin taxe percepute de la furnizorii terți esențiali de servicii TIC vizați.

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

În ceea ce privește utilizarea conform legii, economică, efectivă și eficace a creditelor care rezultă din propunere, se preconizează că propunerea nu va genera riscuri noi semnificative care să nu fie acoperite de un cadru de control intern existent. Cu toate acestea, o nouă provocare ar putea fi legată de asigurarea colectării în timp util a taxelor de la furnizorii terți esențiali de servicii TIC în cauză.

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)

Sistemele de gestiune și de control prevăzute în Regulamentele privind AES sunt deja instituite. AES colaborează îndeaproape cu Serviciul de Audit Intern al Comisiei pentru a se asigura că sunt aplicate normele corespunzătoare în toate domeniile cadrului de control intern. Aceste mecanisme se vor aplica și în ceea ce privește rolul AES în conformitate cu prezenta propunere. În plus, în fiecare exercițiu financiar, Parlamentul European, la recomandarea Consiliului, aprobă fiecărei AES descărcarea de gestiune pentru execuția bugetului.

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.

În scopul combaterii fraudei, a corupției și a altor ilegalități, 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 AES fără nicio restricție. AES dispun de o strategie antifraudă specifică și de un plan de acțiune aferent acesteia. Acțiunile consolidate ale AES în domeniul luptei antifraudă vor fi conforme cu normele și orientările prevăzute de Regulamentul financiar (măsuri antifraudă ca parte a unei bune gestiuni financiare), cu politicile OLAF de prevenire a fraudei, cu dispozițiile prevăzute de Strategia antifraudă a Comisiei [COM(2011)376], precum și cu cele prevăzute în Abordarea comună privind agențiile descentralizate ale UE (iulie 2012) și în foaia de parcurs aferentă. În plus, regulamentele de instituire a AES, precum și regulamentele financiare ale AES stabilesc dispozițiile privind execuția și controlul bugetelor AES și normele financiare aplicabile, inclusiv pe cele care vizează prevenirea fraudei 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)

Linii bugetare existente

<u>În ordinea</u> rubricilor din cadrul financiar multianual și a liniilor bugetare.

Rubrica din cadrul financiar multianual	Linia bugetară	Tipul de cheltuieli	Contribuție			
	Număr	Dif./Nedif.[52].	din partea țărilor AELS[53]	din partea țărilor candidate[54]	din partea țărilor terțe	în sensul articolului 21 alineatul (2) litera (b) din Regulamentul financiar

Noile linii bugetare solicitate

<u>În ordinea</u> rubricilor din cadrul financiar multianual și a liniilor bugetare.

Rubrica din cadrul financiar multianual	Linia bugetară	Tipul de cheltuieli	Contribuție			
	Număr	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

[52] Dif. = credite diferențiate/Nedif. = credite nediferențiate.

[53] AELS: Asociația Europeană a Liberului Schimb.

[54] Țări candidate și, după caz, țări potențial candidate din Balcanii de Vest.

3.2. Impactul estimat asupra cheltuielilor

3.3. Sinteza impactului estimat asupra cheltuielilor

milioane EUR (cu trei zecimale)

Rubrica din cadrul financiar multianual	Număr	Rubrica

DG: <..>			2020	2021	2022	2023	2024	2025	2026	2027	**TOTAL**
	Angajamente	(1)									
	Plăți	(2)									
TOTAL credite pentru DG <>	Angajamente										
	Plăți										

Rubrica din cadrul financiar multianual		

milioane EUR (cu trei zecimale)

		2022	2023	2024	2025	2026	2027	**TOTAL**
DG:								
• Resurse umane								
• Alte cheltuieli administrative<>								
Total DG	Credite							

TOTAL credite în cadrul RUBRICII din cadrul financiar multianual	(Total angajamente = Total plăți)							

milioane EUR (cu trei zecimale) în prețuri constante

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**TOTAL**
TOTAL credite în cadrul RUBRICII 1 din cadrul financiar multianual	Angajamente							
	Plăți							

3.3.1. Impactul estimat asupra creditelor

☑ Propunerea/inițiativa nu implică utilizarea de credite operaționale

☐ Propunerea/inițiativa implică utilizarea de credite operaționale, conform explicațiilor de mai jos:

Credite de angajament în milioane EUR (cu trei zecimale) în prețuri constante

A se indica obiectivele și realizările ⇩			2022		2023		2024		2025		2026		2027		**TOTAL**	
REALIZĂRI																
	Tip[55]	Costuri medii	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr. total	Costuri totale
OBIECTIVUL SPECIFIC NR. 1[56]…																
- Realizare																
Subtotal pentru obiectivul specific nr. 1																
OBIECTIVUL SPECIFIC NR. 2…																
- Realizare																
Subtotal pentru obiectivul specific nr. 2																
COSTURI TOTALE																

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

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

3.3.2. Impactul estimat asupra resurselor umane

3.3.2.1. Sinteză

☐ 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) în prețuri constante

ABE, EIOPA, ESMA	2022	2023	2024	2025	2026	2027	**TOTAL**
Agenți temporari (grade AD)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Agenți temporari (grade AST)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Agenți contractuali							
Experți naționali detașați							
TOTAL	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Cerințe privind personalul (ENI):

ABE, EIOPA, ESMA și SEE	2022	2023	2024	2025	2026	2027	**TOTAL**
Agenți temporari (grade AD) ABE=5, EIOPA=5, ESMA=5	15	15	15	15	15	15	15
Agenți temporari (grade AST) ABE=1, EIOPA=1, EEA=1	3	3	3	3	3	3	3
Agenți contractuali							
Experți naționali detașați							
TOTAL	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. Necesarul de resurse umane estimat pentru DG (sub tutela căreia se află agenția)

☑ Propunerea/inițiativa nu implică utilizarea de resurse umane.

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

Estimarea se exprimă în numere întregi (sau cel mult cu o zecimală)

		2022	2023	2024	2025	2026	2027
• **Posturi din schema de personal (funcționari și agenți temporari)**							
• **Personal extern (în echivalent normă întreagă: ENI)**[57]							
XX 01 02 01 (AC, END, INT din „pachetul global")							
XX 01 02 02 (AC, AL, END, INT și JPD în delegații)							
XX 01 04 ***yy***[58]	- la sediu[59]						
	- în delegații						
XX 01 05 02 (AC, END, INT – cercetare indirectă)							
10 01 05 02 (AC, END, INT – cercetare directă)							
Alte linii bugetare (a se preciza)							
TOTAL							

XX este domeniul de politică sau titlul din buget vizat.

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 cadrul DG-ului, completate, după caz, cu resurse suplimentare ce ar putea fi acordate DG-ului care gestionează acțiunea în cadrul procedurii anuale de alocare și ținând seama de constrângerile bugetare.

Descrierea sarcinilor care trebuie efectuate:

Funcționari și personal temporar	
Personal extern	

Descrierea metodei de calcul al costului pentru unitățile ENI ar trebui inclusă în anexa V secțiunea 3.

57 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.

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

59 În principal pentru fondurile structurale, Fondul european agricol pentru dezvoltare rurală (FEADR) și Fondul european pentru pescuit (FEP).

3.3.3. Compatibilitatea cu actualul cadru financiar multianual

☑ Propunerea/inițiativa este compatibilă cu cadrul financiar multianual actual.

☐ Propunerea/inițiativa va necesita o reprogramare a rubricii corespunzătoare din cadrul financiar multianual.

☐ Propunerea/inițiativa necesită recurgerea la instrumentul de flexibilitate sau la revizuirea cadrului financiar multianual[60].

A se explica necesitatea efectuării acestei acțiuni, precizând rubricile și liniile bugetare în cauză, precum și sumele aferente. […]

3.3.4. Contribuțiile terților

☐ Propunerea/inițiativa nu prevede cofinanțare din partea terților.

☑ Propunerea/inițiativa prevede cofinanțare, estimată după cum urmează:

milioane EUR (cu trei zecimale)

ABE

	2022	2023	2024	2025	2026	2027	Total
Costurile sunt acoperite în proporție de 100 % din taxele percepute de la entitățile supravegheate[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL credite cofinanțate	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Total
Costurile sunt acoperite în proporție de 100 % din taxele percepute de la entitățile supravegheate[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
TOTAL credite cofinanțate	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	Total

60 A se vedea articolele 11 și 17 din Regulamentul (UE, Euratom) nr. 1311/2013 al Consiliului de stabilire a cadrului financiar multianual pentru perioada 2014-2020.

61 100 % din costul total estimat plus contribuțiile integrale ale angajatorului la sistemul de pensii.

62 100 % din costul total estimat plus contribuțiile integrale ale angajatorului la sistemul de pensii.

Costurile sunt acoperite în proporție de 100 % din taxele percepute de la entitățile supravegheate[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL credite cofinanțate	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. 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[64]						
		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 (cf. punctul 1.6)		
Articolul …….								

Pentru veniturile diverse alocate, a se preciza linia bugetară (liniile bugetare) de cheltuieli afectată (afectate).

[…]

A se preciza metoda de calcul a impactului asupra veniturilor.

[…]

63 100 % din costul total estimat plus contribuțiile integrale ale angajatorului la sistemul de pensii.

64 În ceea ce privește resursele proprii tradiționale (taxe vamale, cotizații pentru zahăr), sumele indicate trebuie să fie sume nete, și anume sume brute după deducerea unei cote de 20 % pentru costuri de colectare.

ANEXĂ

Ipoteze generale

Titlul I – Cheltuieli cu personalul

Următoarele ipoteze specifice au fost aplicate la calcularea cheltuielilor cu personalul pe baza necesarului de personal identificat, explicat mai jos:

- Personalul suplimentar angajat în 2022 este calculat pentru o perioadă de 6 luni, având în vedere timpul estimat necesar pentru recrutarea personalului suplimentar.
- Costul mediu anual al unui agent temporar este de 150 000 EUR, incluzând costurile aferente echipării („*habillage*”) (clădiri, IT etc.) în valoare de 25 000 EUR.
- Coeficienții corectori aplicabili salariilor personalului din Paris (ABE și ESMA) și Frankfurt (EIOPA) sunt de 117,7 și, respectiv, 99,4.
- Contribuțiile angajatorului la sistemul de pensii pentru agenții temporari s-au bazat pe salariile standard de bază incluse în costurile anuale medii standard, și anume 95 660 EUR.
- Agenții temporari suplimentari sunt AD5 și AST.

Titlul II – Cheltuieli de infrastructură și de funcționare

Costurile se bazează pe înmulțirea numărului de membri ai personalului cu procentul din an cât sunt angajați și cu costul standard aferent echipării („*habillage*”), mai exact 25 000 EUR.

Titlul III – Cheltuieli operaționale

Costurile sunt estimate sub rezerva următoarelor ipoteze:

- Costurile de traducere sunt stabilite la 350 000 EUR pe an pentru fiecare AES
- Se presupune că respectivele costuri IT punctuale de 500 000 EUR pe AES vor fi puse în aplicare pe parcursul celor doi ani 2022 și 2023, pe baza unei divizări de 50 % – 50 %. Costurile anuale de întreținere începând cu 2024 sunt estimate la 50 000 EUR pe AES
- Costurile anuale cu supravegherea la fața locului sunt estimate la 200 000 EUR pe AES.

Estimările prezentate mai sus au drept rezultat următoarele costuri pe an:

Rubrica din cadrul financiar multianual	Număr	

Prețuri constante

ABE:			2022	2023	2024	2025	2026	2027	**TOTAL**
Titlul 1:	Angajamente	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Plăți	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Titlul 2:	Angajamente	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Plăți	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Titlul 3:	Angajamente	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Plăți	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAL credite pentru ABE	Angajamente	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Plăți	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA:			2022	2023	2024	2025	2026	2027	**TOTAL**
Titlul 1:	Angajamente	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Plăți	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Titlul 2:	Angajamente	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Plăți	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Titlul 3:	Angajamente	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Plăți	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAL credite	Angajamente	=1+1a +3a	1,305	1,811	1,611	1,611	1,611	1,611	9,560

pentru EIOPA	Plăți	=2+2a +3b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA:			2022	2023	2024	2025	2026	2027	**TOTAL**
Titlul 1:	Angajamente	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Plăți	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Titlul 2:	Angajamente	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Plăți	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Titlul 3:	Angajamente	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Plăți	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAL credite pentru ESMA	Angajamente	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Plăți	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Propunerea/inițiativa implică utilizarea de credite operaționale, conform explicațiilor de mai jos:

Credite de angajament în milioane EUR (cu trei zecimale) în prețuri constante

ABE

A se indica obiectivele și realizările ⇩			2022		2023		2024		2025		2026		2027			
	REALIZĂRI															
	Tip[65]	Costuri medii	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr. total	Costuri totale
Obiectivul SPECIFIC NR. 1[66] Supravegherea directă a furnizorilor terți esențiali de servicii TIC																
- Realizare				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Subtotal pentru obiectivul specific nr. 1																
OBIECTIVUL SPECIFIC NR. 2…																
- Realizare																
Subtotal pentru obiectivul specific nr. 2																
COSTURI TOTALE				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

EIOPA

A se indica obiectivele și realizările ⇩			2022		2023		2024		2025		2026		2027			
	REALIZĂRI															
	Tip[67]	Costuri medii	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr. total	Costuri totale
Obiectivul SPECIFIC NR. 1[68] Supravegherea directă a furnizorilor terți esențiali de servicii TIC																
- Realizare				0,800		0,800		0,600		0,600		0,600		0,600		4,000

65 Realizările se referă la produsele și serviciile care vor fi furnizate (de exemplu: numărul de schimburi de studenți finanțate, numărul de km de drumuri construiți etc.).

66 Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”.

67 Realizările se referă la produsele și serviciile care vor fi furnizate (de exemplu: numărul de schimburi de studenți finanțate, numărul de km de drumuri construiți etc.).

68 Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”.

Subtotal pentru obiectivul specific nr. 1															
OBIECTIVUL SPECIFIC NR. 2…															
- Realizare															
Subtotal pentru obiectivul specific nr. 2															
COSTURI TOTALE		**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

ESMA

A se indica obiectivele și realizările ⇩			2022		2023		2024		2025		2026		2027			
	REALIZĂRI															
	Tip[69]	Costuri medii	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr. total	Costuri totale
Obiectivul SPECIFIC NR. 1[70] Supravegherea directă a furnizorilor terți esențiali de servicii TIC																
- Realizare				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Subtotal pentru obiectivul specific nr. 1																
OBIECTIVUL SPECIFIC NR. 2…																
- Realizare																
Subtotal pentru obiectivul specific nr. 2																
COSTURI TOTALE				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

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

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

Activitățile de supraveghere sunt finanțate integral din taxele percepute de la entitățile supravegheate, după cum urmează:

ABE

	2022	2023	2024	2025	2026	2027	Total
Costurile sunt acoperite în proporție de 100 % din taxele percepute de la entitățile supravegheate[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL credite cofinanțate	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Total
Costurile sunt acoperite în proporție de 100 % din taxele percepute de la entitățile supravegheate[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
TOTAL credite cofinanțate	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	Total
Costurile sunt acoperite în proporție de 100 % din taxele percepute de la entitățile supravegheate[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL credite cofinanțate	1,373	1,948	1,748	1,748	1,748	1,748	10,313

INFORMAȚII SPECIFICE

Competențele privind supravegherea directă

Ca o introducere, ar trebui reamintit faptul că entitățile care fac obiectul supravegherii directe de către ESMA ar trebui să plătească taxele către ESMA (costuri punctuale pentru înregistrare și costuri

[71] 100 % din costul total estimat plus contribuțiile integrale ale angajatorului la sistemul de pensii.
[72] 100 % din costul total estimat plus contribuțiile integrale ale angajatorului la sistemul de pensii.
[73] 100 % din costul total estimat plus contribuțiile integrale ale angajatorului la sistemul de pensii.

recurente pentru supravegherea continuă). Acesta este cazul agențiilor de rating de credit [a se vedea Regulamentul delegat (UE) nr. 272/2012 al Comisiei] și al registrelor centrale de tranzacții [Regulamentul delegat (UE) nr. 1003/2013 al Comisiei].

În temeiul prezentei propuneri legislative, AES li se vor încredința noi sarcini menite să promoveze convergența abordărilor în materie de supraveghere a riscurilor TIC generate de părți terțe în sectorul financiar, prin aplicarea unui cadru de supraveghere la nivelul Uniunii în cazul furnizorilor terți esențiali de servicii TIC.

Cadrul de supraveghere preconizat de prezenta propunere se bazează pe arhitectura instituțională existentă în domeniul serviciilor financiare, prin care Comitetul comun al AES asigură coordonarea transsectorială în ceea ce privește toate aspectele legate de riscurile TIC, în conformitate cu sarcinile care îi revin în materie de securitate cibernetică, cu sprijinul subcomitetului relevant (Forumul de supraveghere), care desfășoară activități pregătitoare pentru decizii individuale și recomandări colective adresate furnizorilor terți esențiali de servicii TIC.

Prin acest cadru, AES desemnate drept supraveghetori principali pentru fiecare furnizor terț esențial de servicii TIC sunt învestite cu competențe pentru a se asigura că furnizorii de servicii tehnologice care îndeplinesc un rol esențial în funcționarea sectorului financiar sunt monitorizați în mod adecvat la o scară paneuropeană. Sarcinile de supraveghere sunt stabilite în propunere și clarificate în continuare în expunerea de motive. Acestea includ dreptul de a solicita toate informațiile și documentele relevante pentru a efectua investigații și inspecții generale, dreptul de a adresa recomandări și, prin urmare, de a prezenta rapoarte cu privire la acțiunile întreprinse sau la măsurile corective puse în aplicare în legătură cu recomandările respective.

Pentru a îndeplini noile sarcini prevăzute de prezenta propunere, AES angajează, prin urmare, personal suplimentar care este specializat în domeniul riscurilor TIC și se axează pe evaluarea dependențelor de părți terțe.

Necesarul de resurse umane poate fi estimat la 6 ENI pentru fiecare autoritate (5 AD și 1 AST care să acorde asistență pentru AD). De asemenea, AES vor suporta costuri IT suplimentare, estimate la 500 000 EUR (costuri punctuale), precum și 50 000 EUR pe an pentru fiecare dintre cele trei AES pentru costurile de întreținere. Un element important în îndeplinirea noilor sarcini constă în misiunile de inspecție și audit la fața locului, care pot fi estimate la 200 000 EUR pe an pentru fiecare AES. Costurile de traducere pentru diferitele documente pe care AES le-ar primi de la furnizorii terți esențiali de servicii TIC sunt, de asemenea, incluse la rândul privind costurile operaționale și reprezintă 350 000 EUR pe an.

Toate costurile administrative menționate mai sus vor fi finanțate integral din taxele anuale percepute de AES de la furnizorii terți esențiali de servicii TIC supravegheați (fără impact asupra bugetului UE).