I

*(Acte legislative)*

# REGULAMENTE

## REGULAMENTUL (UE) 2022/2554 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

**din 14 decembrie 2022**

**privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011**

**(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 ([1]),

având în vedere avizul Comitetului Economic și Social European ([2]),

hotărând în conformitate cu procedura legislativă ordinară ([3]),

întrucât:

(1) În era digitală, tehnologia informației și a comunicațiilor (TIC) sprijină sistemele complexe utilizate pentru activitățile de zi cu zi. Aceasta susține activitatea economiilor noastre în sectoare-cheie, inclusiv în sectorul financiar, și îmbunătățește funcționarea pieței interne. 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 extensivă a sistemelor TIC și gradul ridicat de digitalizare și conectivitate sunt în prezent caracteristicile de bază ale activităților entităților financiare din Uniune, reziliența digitală a acestora trebuie încă să fie mai bine abordată și integrată în cadrele lor operaționale mai ample.

(2) În ultimele decenii, utilizarea TIC a dobândit un rol esențial în furnizarea serviciilor financiare, ajungând în prezent să aibă o importanță critică în ceea ce privește operarea funcțiilor zilnice uzuale ale tuturor entităților financiare. Astăzi, 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, creditarea de la persoană la persoană, ratingul de credit, gestionarea creanțelor și operațiunile de tip back-office. Sectorul asigurărilor a fost, de

([1]) JO C 343, 26.8.2021, p. 1.
([2]) JO C 155, 30.4.2021, p. 38.
([3]) Poziția Parlamentului European din 10 noiembrie 2022 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 28 noiembrie 2022.

asemenea, transformat prin utilizarea TIC, de la apariția intermediarilor de asigurări care își oferă serviciile online folosind InsurTech, până la subscrierea de asigurări folosind mijloace digitale. Finanțele nu numai că au devenit în mare parte digitale în întregul sector, ci digitalizarea a aprofundat, de asemenea, interconexiunile și dependențele din interiorul sectorului financiar, precum și relaționarea cu furnizorii terți de infrastructură și servicii.

(3) Comitetul european pentru risc sistemic (CERS) a reafirmat într-un raport din 2020 care abordează riscul cibernetic sistemic modul în care nivelul ridicat existent de interconectare dintre entitățile financiare, piețele financiare și infrastructurile pieței financiare și, în special, interdependențele dintre sistemele lor TIC ar putea constitui o vulnerabilitate sistemică, deoarece incidentele cibernetice localizate s-ar putea răspândi rapid de la oricare dintre cele aproximativ 22 000 de entități financiare ale Uniunii la întregul sistem financiar, nestingherite de limitele geografice. Breșele grave de securitate a TIC care au loc în sectorul financiar 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, cum ar fi generarea de 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 și internațional, precum și de la nivelul Uniunii, într-o încercare de a spori reziliența digitală, a stabili standarde și a coordona activitatea de reglementare sau de supraveghere. La nivel internațional, Comitetul de la Basel pentru supraveghere bancară, Comitetul pentru plăți și infrastructuri de piață, Consiliul pentru Stabilitate Financiară, Institutul pentru Stabilitate Financiară, precum și G7 și G20 urmăresc să furnizeze autorităților competente și operatorilor pe piață din diferite jurisdicții instrumente care să consolideze reziliența sistemelor lor financiare. Această activitate a fost determinată, de asemenea, de necesitatea de a lua în considerare în mod corespunzător riscurile TIC în contextul unui sistem financiar global foarte interconectat și de a urmări o mai mare coerență a bunelor practici relevante.

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

(6) În Comunicarea sa din 8 martie 2018 intitulată „Planul de acțiune privind FinTech: pentru un sector financiar european mai competitiv și mai inovator”, Comisia a evidențiat importanța capitală a creșterii rezilienței sectorului financiar al Uniunii, inclusiv din punct de vedere operațional, pentru a asigura siguranța tehnologică și buna sa funcționare, recuperarea rapidă în urma unor breșe și incidente legate de TIC, permițând în cele din urmă furnizarea eficace și fără probleme a serviciilor financiare în întreaga Uniune, inclusiv în situații de criză, și menținând totodată încrederea consumatorilor și a pieței.

(7) În aprilie 2019, Autoritatea europeană de supraveghere (Autoritatea bancară europeană, ABE), instituită prin Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului ([4]), Autoritatea europeană de supraveghere (Autoritatea europeană de asigurări și pensii ocupaționale, EIOPA), instituită prin Regulamentul (UE) nr. 1094/2010 al Parlamentului European și al Consiliului ([5]), și Autoritatea europeană de supraveghere (Autoritatea europeană pentru valori mobiliare și piețe, ESMA), instituită prin Regulamentul (UE) nr. 1095/2010 al Parlamentului

([4]) Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea bancară europeană), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/78/CE a Comisiei (JO L 331, 15.12.2010, p. 12).

([5]) Regulamentul (UE) nr. 1094/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea europeană de asigurări și pensii ocupaționale), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/79/CE a Comisiei (JO L 331, 15.12.2010, p. 48).

European și al Consiliului ([6]) (cunoscute în mod colectiv drept „autoritățile europene de supraveghere" sau „AES"), au emis în comun un aviz tehnic solicitând o abordare coerentă a riscurilor TIC în domeniul financiar și recomandând consolidarea, în mod proporțional, a rezilienței operaționale digitale a sectorului serviciilor financiare prin intermediul unei inițiative sectoriale a Uniunii.

(8) Sectorul financiar al Uniunii este reglementat printr-un cadru unic de reglementare 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 reziliența operațională digitală, prin consolidarea mandatelor autorităților competente pentru a le permite să supravegheze gestionarea riscurilor TIC în sectorul financiar în vederea protejării integrității și eficienței pieței interne și pentru facilitarea funcționării organizate a acesteia.

(9) Disparitățile legislative și abordările naționale inegale în materie de reglementare sau de supraveghere cu privire la riscurile TIC generează obstacole în calea funcționării pieței interne a serviciilor financiare, împiedicând exercitarea fără probleme a libertății de stabilire și de prestare de servicii pentru entitățile financiare care desfășoară activități transfrontaliere. Concurența între entități financiare de același tip care operează în diferite state membre ar putea, de asemenea, să fie denaturată. Acest lucru este valabil în special în domeniile în care armonizarea la nivelul Uniunii a fost foarte limitată, cum ar fi testarea rezilienței operaționale digitale, sau a lipsit, cum ar fi monitorizarea riscurilor TIC generate de părți terțe. Disparitățile care decurg din evoluțiile preconizate la nivel național ar putea genera noi obstacole în calea funcționării pieței interne, în detrimentul participanților la piață și al stabilității financiare.

(10) Până în prezent, întrucât dispozițiile legate de riscurile TIC au fost abordate doar parțial la nivelul Uniunii, există lacune sau suprapuneri în domenii importante, cum ar fi raportarea incidentelor legate de TIC și testarea rezilienței operaționale digitale, precum și inconsecvențe ca urmare a apariției unor norme naționale divergente sau a aplicării ineficiente din punctul de vedere al costurilor a normelor care se suprapun. Acest lucru este în special în detrimentul domeniilor care utilizează intensiv TIC, precum sectorul financiar, 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 acestea 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 negative 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 suplimentară a principalelor cerințe privind reziliența operațională digitală a tuturor entităților financiare. Dezvoltarea capacităților TIC și a rezilienței generale a entităților financiare, pe baza unor astfel de cerințe principale, în scopul de 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 interne, prezentul regulament ar trebui să se bazeze pe dispozițiile articolului 114 din Tratatul privind funcționarea Uniunii Europene (TFUE), astfel cum au fost interpretate în conformitate cu jurisprudența constantă a Curții de Justiție a Uniunii Europene (denumită în continuare „Curtea de Justiție").

(12) Prezentul regulament urmărește să consolideze și să actualizeze cerințele privind riscurile TIC ca parte a cerințelor privind riscurile operaționale care, până în prezent, au fost abordate separat în diferite acte juridice ale Uniunii. 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 respective nu au abordat în mod cuprinzător, la momentul adoptării lor, toate componentele rezilienței operaționale. Atunci când au fost dezvoltate într-o mai mare măsură în actele juridice respective ale Uniunii, normele 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

([6]) Regulamentul (UE) nr. 1095/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea europeană pentru valori mobiliare și piețe), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/77/CE a Comisiei (JO L 331, 15.12.2010, p. 84).

degrabă decât norme calitative specifice pentru protecția, detectarea, limitarea, recuperarea și repararea capacităților în cazul unor incidente legate de TIC sau referitoare la capacitățile de raportare și de testare digitală. Actele respective erau menite, în principal, să acopere și să actualizeze norme esențiale privind supravegherea prudențială, integritatea pieței sau conduita pe piață. Prin consolidarea și actualizarea diferitelor norme privind riscurile TIC, toate dispozițiile care abordează riscul digital în sectorul financiar ar urma să fie reunite pentru prima dată, într-un mod coerent, într-un singur act legislativ. Prin urmare, prezentul regulament elimină lacunele sau remediază inconsecvențele din unele dintre actele juridice anterioare, inclusiv în ceea ce privește terminologia utilizată în acestea, și face trimiteri explicite la riscurile TIC prin intermediul unor norme specifice privind capacitățile de gestionare a riscurilor TIC, raportarea incidentelor, testarea rezilienței operaționale și monitorizarea riscurilor TIC generate de părți terțe. Astfel, prezentul regulament ar trebui, de asemenea, să crească gradul de conștientizare cu privire la riscurile TIC și să recunoască faptul că incidentele legate de TIC și o lipsă de reziliență operațională ar putea periclita soliditatea entităților financiare.

(13) Entitățile financiare ar trebui să aibă aceeași abordare și să respecte aceleași norme bazate pe principii cu privire la riscurile TIC, ținând cont de dimensiunea și profilul lor general de risc și de natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor. Consecvența contribuie la creșterea încrederii în sistemul financiar și la menținerea stabilității acestuia, în special în perioade de dependență ridicată de sisteme, platforme și infrastructuri 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) Un regulament ajută la reducerea complexității reglementării, favorizează convergența supravegherii și sporește securitatea juridică, contribuind totodată la limitarea costurilor de asigurare a conformității, în special pentru entitățile financiare care desfășoară activități transfrontaliere, precum și la reducerea denaturărilor concurenței. Prin urmare, opțiunea pentru un regulament în vederea instituirii unui cadru comun pentru reziliența operațională digitală a entităților financiare reprezintă cel mai adecvat mod de a garanta o aplicare omogenă și coerentă a tuturor componentelor gestionării riscurilor TIC de către sectorul financiar al Uniunii.

(15) Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului ([7]) a fost primul cadru de reglementare orizontal în materie de securitate cibernetică adoptat la nivelul Uniunii, care se aplică și în cazul a trei tipuri de entități financiare, și anume instituțiile de credit, locurile de tranzacționare și contrapărțile centrale. Totuși, întrucât Directiva (UE) 2016/1148 a stabilit un mecanism de identificare la nivel național a operatorilor de servicii esențiale, doar anumite instituții de credit, locuri de tranzacționare și contrapărți centrale care au fost identificate de statele membre au fost, în practică, incluse în domeniul său de aplicare, trebuind, prin urmare, să respecte cerințele privind securitatea TIC și notificarea incidentelor prevăzute în aceasta. Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului ([8]) stabilește un criteriu uniform pentru a determina entitățile care intră în domeniul său de aplicare (regula privind criteriul de dimensiune), menținând în același timp în domeniul său de aplicare cele trei tipuri de entități financiare.

(16) Cu toate acestea, întrucât prezentul regulament sporește nivelul de armonizare în ceea ce privește diferitele componente ale rezilienței digitale, prin introducerea unor cerințe privind gestionarea riscurilor TIC și raportarea incidentelor legate de TIC care sunt mai stricte în comparație cu cele prevăzute în dreptul actual al Uniunii privind serviciile financiare, acest nivel sporit constituie o armonizare sporită și în comparație cu cerințele prevăzute în Directiva (UE) 2022/2555. Prin urmare, prezentul regulament constituie *lex specialis* în raport cu Directiva (UE) 2022/2555. În același timp, este esențial să se mențină o legătură puternică între sectorul financiar și cadrul orizontal de securitate cibernetică al Uniunii, astfel cum este prevăzut în prezent în Directiva (UE) 2022/2555, pentru a asigura coerența cu strategiile de securitate cibernetică adoptate de statele membre și pentru a permite autorităților de supraveghere financiară să fie informate cu privire la incidentele cibernetice care afectează alte sectoare care intră sub incidența directivei respective.

([7]) 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).

([8]) Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (a se vedea pagina 80 din prezentul Jurnal Oficial).

(17) În conformitate cu articolul 4 alineatul (2) din Tratatul privind Uniunea Europeană și fără a aduce atingere controlului jurisdicțional exercitat de Curtea de Justiție, prezentul regulament nu ar trebui să aducă atingere responsabilității statelor membre cu privire la funcțiile esențiale ale statului în ceea ce privește siguranța publică, apărarea și protejarea securității naționale, de exemplu în ceea ce privește furnizarea de informații care ar fi contrare protejării securității naționale.

(18) Pentru a facilita procesul de învățare transsectorială și pentru a valorifica în mod eficace experiențele altor sectoare în abordarea amenințărilor cibernetice, entitățile financiare menționate în Directiva (UE) 2022/2555 ar trebui să rămână parte a „ecosistemului" directivei respective [de exemplu, Grupul de cooperare și echipele de intervenție în caz de incidente de securitate informatică (echipe CSIRT)]. AES și autoritățile naționale competente ar trebui să poată participa la discuțiile de politică strategice și la lucrările tehnice ale Grupului de cooperare în temeiul directivei respective și să schimbe informații, precum și să coopereze în continuare cu punctele unice de contact desemnate sau instituite în conformitate cu directiva respectivă. Autoritățile competente în temeiul prezentului regulament ar trebui, de asemenea, să se consulte și să coopereze cu echipele CSIRT. Autoritățile competente ar trebui, de asemenea, să fie în măsură să solicite consultanță tehnică din partea autorităților competente desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555 și să stabilească acorduri de cooperare menite să asigure mecanisme eficace și rapide de coordonare a răspunsului.

(19) Având în vedere legăturile puternice dintre reziliența digitală și reziliența fizică a entităților financiare, este necesară o abordare coerentă în ceea ce privește reziliența entităților critice în prezentul regulament și în Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului ([9]). Având în vedere că reziliența fizică a entităților financiare este abordată în mod cuprinzător de obligațiile de gestionare a riscurilor TIC și de raportare care fac obiectul prezentului regulament, obligațiile prevăzute în capitolele III și IV din Directiva (UE) 2022/2557 nu ar trebui să se aplice entităților financiare care intră în domeniul de aplicare al directivei respective.

(20) Furnizorii de servicii de cloud computing sunt o categorie de infrastructuri digitale care intră sub incidența Directivei (UE) 2022/2555. Cadrul de supraveghere al Uniunii (denumit în continuare „cadrul de supraveghere") instituit prin prezentul regulament se aplică tuturor furnizorilor terți esențiali de servicii TIC, inclusiv furnizorilor de servicii de cloud computing care furnizează servicii TIC entităților financiare, și ar trebui să fie considerat complementar supravegherii în temeiul Directivei (UE) 2022/2555. 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 instituie o autoritate de supraveghere digitală.

(21) Pentru a păstra controlul deplin asupra riscurilor TIC, entitățile financiare trebuie să dispună de capacități cuprinzătoare care să permită o gestionare sănătoasă și eficace a riscurilor TIC, precum și de mecanisme și politici specifice pentru tratarea tuturor incidentelor legate de TIC și pentru raportarea incidentelor majore legate de TIC. De asemenea, entitățile financiare ar trebui să dispună de politici pentru testarea sistemelor, controalelor și proceselor TIC, precum și pentru gestionarea riscurilor TIC generate de părți terțe. Nivelul de referință al rezilienței operaționale digitale pentru entitățile financiare ar trebui să fie majorat, permițând totodată o aplicare proporțională a cerințelor pentru anumite entități financiare, în special pentru microîntreprinderi, precum și pentru entitățile financiare care fac obiectul unui cadru simplificat de gestionare a riscurilor TIC. Pentru a facilita o supraveghere eficientă a instituțiilor pentru furnizarea de pensii ocupaționale care să fie proporțională și să abordeze necesitatea de a reduce sarcinile administrative ale autorităților competente, mecanismele naționale de supraveghere relevante cu privire la astfel de entități financiare ar trebui să țină seama de dimensiunea și profilul general de risc al acestora, precum și de natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor, chiar și atunci când pragurile relevante stabilite la articolul 5 din Directiva (UE) 2016/2341 a Parlamentului European și a Consiliului ([10]) sunt depășite. În special, activitățile de supraveghere ar trebui să se concentreze în primul rând asupra necesității de a aborda riscurile grave asociate gestionării riscurilor TIC ale unei anumite entități.

([9]) Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului (a se vedea pagina 164 din prezentul Jurnal Oficial).

([10]) Directiva (UE) 2016/2341 a Parlamentului European și a Consiliului din 14 decembrie 2016 privind activitățile și supravegherea instituțiilor pentru furnizarea de pensii ocupaționale (IORP) (JO L 354, 23.12.2016, p. 37).

Autoritățile competente ar trebui, de asemenea, să mențină o abordare vigilentă, dar proporțională, în ceea ce privește supravegherea instituțiilor pentru furnizarea de pensii ocupaționale care, în conformitate cu articolul 31 din Directiva (UE) 2016/2341, externalizează către furnizorii de servicii o parte semnificativă a activității lor principale, cum ar fi gestionarea activelor, calculele actuariale, contabilitatea și gestionarea datelor.

(22) 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) instituită prin Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului ([11]) și de Grupul de cooperare în temeiul Directivei (UE) 2022/2555, încă există sau pot apărea abordări divergente privind stabilirea pragurilor și folosirea taxonomiilor pentru restul entităților financiare. Din cauza divergențelor respective, există cerințe multiple pe care entitățile financiare trebuie să le respecte, în special atunci când își desfășoară activitatea în mai multe state membre și când fac parte dintr-un grup financiar. În plus, astfel de divergențe pot împiedica crearea unor noi mecanisme uniforme sau centralizate ale Uniunii, care să accelereze procesul de raportare și să sprijine un schimb de informații rapid și fără probleme între autoritățile competente, care este esențial pentru abordarea riscurilor TIC în cazul unor atacuri la scară largă cu potențiale consecințe sistemice.

(23) Pentru a reduce sarcina administrativă și eventualele obligații de raportare redundante pentru anumite entități financiare, cerința de raportare a incidentelor în temeiul Directivei (UE) 2015/2366 a Parlamentului European și a Consiliului ([12]) ar trebui să înceteze să se aplice furnizorilor de servicii de plată care intră în domeniul de aplicare al prezentului regulament. În consecință, instituțiile de credit, instituțiile emitente de monedă electronică, instituțiile de plată și prestatorii de servicii de informare cu privire la conturi, astfel cum se menționează la articolul 33 alineatul (1) din directiva respectivă, ar trebui, de la data aplicării prezentului regulament, să raporteze în temeiul prezentului regulament toate incidentele operaționale sau de securitate legate de plăți care au fost raportate anterior în temeiul directivei respective, indiferent dacă astfel de incidente sunt legate de TIC sau nu.

(24) Pentru a permite autorităților competente să îndeplinească roluri de supraveghere prin obținerea unei imagini de ansamblu complete asupra naturii, frecvenței, importanței și impactului incidentelor legate de TIC și pentru a consolida schimbul de informații între autoritățile publice relevante, inclusiv autoritățile de aplicare a legii și autoritățile de rezoluție, prezentul regulament ar trebui să prevadă un regim solid de raportare a incidentelor legate de TIC, ale cărui cerințe relevante să remedieze lacunele actuale din dreptul privind serviciile financiare și să elimine suprapunerile și dublările existente, pentru a reduce costurile. Este esențial să se armonizeze regimul de raportare a incidentelor legate de TIC prin impunerea obligației ca toate entitățile financiare să raporteze autorităților lor competente printr-un cadru unic simplificat, astfel cum este prevăzut în prezentul regulament. În plus, AES ar trebui să fie împuternicite să detalieze într-o mai mare măsură elementele relevante pentru cadrul de raportare a incidentelor legate de TIC, cum ar fi taxonomia, intervalele de timp, seturile de date, modelele și pragurile aplicabile. Pentru a asigura coerența deplină cu Directiva (UE) 2022/2555, entităților financiare ar trebui să li se permită, în mod voluntar, să notifice autorității competente relevante amenințările cibernetice semnificative, atunci când consideră că amenințarea cibernetică este relevantă pentru sistemul financiar, pentru utilizatorii serviciilor sau pentru clienți.

(25) În anumite subsectoare financiare au fost elaborate cerințe de testare a rezilienței operaționale digitale care stabilesc cadre de reglementare care nu sunt întotdeauna pe deplin aliniate. Acest lucru conduce la o eventuală duplicare a costurilor pentru entitățile financiare transfrontaliere și face ca recunoașterea reciprocă a rezultatelor testării rezilienței operaționale digitale să devină complexă, ceea ce, la rândul său, poate fragmenta piața internă.

([11]) 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).

([12]) Directiva (UE) 2015/2366 a Parlamentului European și a Consiliului din 25 noiembrie 2015 privind serviciile de plată în cadrul pieței interne, de modificare a Directivelor 2002/65/CE, 2009/110/CE și 2013/36/UE și a Regulamentului (UE) nr. 1093/2010, și de abrogare a Directivei 2007/64/CE (JO L 337, 23.12.2015, p. 35).

(26) În plus, în cazul în care nu este necesară testarea TIC, vulnerabilitățile rămân nedetectate și conduc la expunerea unei entități financiare la riscuri TIC și, în cele din urmă, creează un risc mai mare pentru stabilitatea și integritatea sectorului financiar. Fără intervenția Uniunii, testarea rezilienței operaționale digitale ar continua să fie inconsecventă și nu ar exista un sistem de recunoaștere reciprocă a rezultatelor testelor TIC între diferite jurisdicții. În plus, întrucât este puțin probabil ca alte subsectoare financiare să adopte sistemele de testare la o scară semnificativă, acestea nu s-ar bucura de beneficiile potențiale ale unui cadru de testare, în ceea ce privește dezvăluirea vulnerabilităților și a riscurilor TIC, și testarea capacităților de apărare și a continuității activității, ceea ce contribuie la creșterea încrederii consumatorilor, a furnizorilor și a partenerilor de afaceri. Pentru a remedia aceste suprapuneri, divergențe și lacune, este necesar să se stabilească norme pentru un sistem de testare coordonat, facilitând astfel recunoașterea reciprocă a testelor avansate pentru entitățile financiare care îndeplinesc criteriile stabilite în prezentul regulament.

(27) Dependența entităților financiare de folosirea serviciilor 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 au fost în continuă evoluție în ultimii ani, conducând la o reducere a costurilor în ceea ce privește intermedierea financiară, permițând dezvoltarea și scalabilitatea activităților financiare și oferind în același timp o gamă largă de instrumente TIC pentru gestionarea proceselor interne complexe.

(28) Utilizarea amplă a serviciilor TIC este demonstrată prin acorduri contractuale complexe, în cadrul cărora entitățile financiare se confruntă adesea cu dificultăți în ceea ce privește negocierea unor condiții contractuale care să fie adaptate la standardele prudențiale sau la alte cerințe de reglementare pe care trebuie să le respecte, sau, pe de altă parte, în exercitarea unor drepturi specifice, cum ar fi drepturile de acces sau de audit, chiar și atunci când acestea din urmă sunt consacrate în acordurile contractuale. În plus, multe dintre respectivele acorduri contractuale nu oferă garanții suficiente care să permită monitorizarea 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 acorduri contractuale nu răspund întotdeauna în mod adecvat nevoilor individuale sau specifice ale actorilor din sectorul financiar.

(29) Chiar dacă dreptul Uniunii privind serviciile financiare conține anumite norme generale privind externalizarea, monitorizarea dimensiunii contractuale nu este pe deplin ancorată în dreptul 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, care sunt deosebit de importante atunci când entitățile financiare recurg la furnizori terți de servicii TIC care să sprijine îndeplinirea funcțiilor critice sau importante ale entităților financiare. Aceste principii ar trebui să fie însoțite de un set de drepturi contractuale de bază în legătură cu mai multe elemente legate de executarea și încetarea acordurilor contractuale, cu scopul de a oferi anumite garanții minime care să consolideze capacitatea entităților financiare de a monitoriza în mod eficace toate riscurile TIC care apar la nivelul furnizorilor terți de servicii TIC. Aceste principii sunt complementare legislației sectoriale aplicabile externalizării.

(30) În prezent, este evidentă o anumită lipsă de omogenitate și convergență în ceea ce privește monitorizarea riscurilor TIC generate de părți terțe și a dependențelor TIC față de terți. În pofida eforturilor de abordare a externalizării, cum ar fi Ghidul ABE din 2019 privind externalizarea și Orientările ESMA din 2021 privind externalizarea către furnizorii de servicii de cloud, problema mai amplă a contracarării riscului sistemic care poate fi declanșat de expunerea sectorului financiar la un număr limitat de furnizori terți esențiali de servicii TIC nu este abordată în mod suficient de dreptul Uniunii. Lipsa reglementărilor la nivelul Uniunii este agravată de absența unor norme naționale privind mandatele și instrumentele care să permită autorităților de supraveghere financiară să dobândească o bună înțelegere a dependențelor TIC față de terți și să monitorizeze în mod adecvat riscurile care decurg din concentrarea dependențelor TIC față de terți.

(31) 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 capacității mecanismelor naționale de a oferi autorităților de supraveghere financiară instrumente adecvate pentru 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, care să permită o monitorizare continuă a activităților furnizorilor terți de servicii TIC care sunt furnizori terți esențiali de servicii TIC pentru entitățile financiare, asigurând în același timp păstrarea confidențialității și a securității clienților, alții decât entitățile financiare. Deși furnizarea de servicii TIC intragrup implică riscuri și beneficii specifice, aceasta nu ar trebui considerată în mod automat mai puțin riscantă decât furnizarea de servicii TIC de către furnizorii din afara unui grup financiar și, prin urmare, ar trebui să facă obiectul aceluiași cadru de reglementare. Cu toate acestea, atunci când serviciile TIC sunt furnizate în interiorul aceluiași grup financiar, entitățile financiare ar putea avea un nivel mai ridicat de control asupra furnizorilor intragrup, de care ar trebui să se țină seama în evaluarea globală a riscurilor.

(32) Având în vedere că riscurile TIC devin din ce în ce mai complexe și mai sofisticate, măsurile adecvate pentru detectarea și prevenirea riscurilor TIC depind în mare măsură de schimbul periodic între entitățile financiare de informații privind amenințările și vulnerabilitatea. Schimbul de informații contribuie la crearea unui grad sporit de conștientizare cu privire la amenințările cibernetice. La rândul său, acest lucru sporește capacitatea entităților financiare de a preveni ca amenințările cibernetice să devină incidente reale legate de TIC și permite entităților financiare să limiteze mai eficient impactul incidentelor legate de TIC și să se redreseze mai rapid. În absența unor orientări la nivelul Uniunii, mai mulți factori par să fi împiedicat astfel de schimburi de informații, în special incertitudinea cu privire la compatibilitatea cu normele privind protecția datelor, cu normele antitrust și cu cele privind răspunderea.

(33) În plus, incertitudinile cu privire la tipul de informații care pot fi partajate cu alți participanți pe piață sau cu autorități care nu au atribuții de supraveghere (precum ENISA, pentru contribuții analitice sau Europolul, în scopul asigurării respectării legii) conduc la nedivulgarea de informații utile. Prin urmare, amploarea și calitatea schimbului de informații rămân în prezent limitate și fragmentate, schimburile relevante fiind realizate în cea mai mare parte la nivel local (prin inițiative naționale) și fără acorduri consecvente de schimburi de informații la nivelul Uniunii, adaptate nevoilor unui sistem financiar integrat. Prin urmare, este important să se consolideze aceste canale de comunicare.

(34) Entitățile financiare ar trebui să fie încurajate să facă schimb de informații și date operative privind amenințările cibernetice și să își valorifice în mod colectiv cunoștințele individuale și experiența practică la nivel strategic, tactic și operațional, în vederea consolidării capacităților lor de a evalua, a monitoriza, a apăra împotriva amenințărilor cibernetice și a răspunde în mod adecvat la acestea, prin participarea la acorduri privind schimbul de informații. Prin urmare, este necesar să se favorizeze apariția la nivelul Uniunii a unor mecanisme pentru acorduri voluntare privind schimbul de informații care, atunci când au loc în medii de încredere, ar ajuta comunitatea industriei financiare să prevină amenințările cibernetice și să răspundă în mod colectiv la acestea prin limitarea rapidă a răspândirii riscurilor TIC și prin împiedicarea unei contaminări potențiale prin canalele financiare. Aceste mecanisme ar trebui să respecte normele Uniunii aplicabile în domeniul concurenței din Comunicarea Comisiei din 14 ianuarie 2011 intitulată „Orientări privind aplicabilitatea articolului 101 din Tratatul privind funcționarea Uniunii Europene acordurilor de cooperare orizontală”, precum și normele Uniunii în materie de protecție a datelor, în special Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([13]). Acestea ar trebui să funcționeze pe baza utilizării unuia sau a mai multor temeiuri juridice prevăzute la articolul 6 din regulamentul respectiv, cum ar fi în contextul prelucrării datelor cu caracter personal care este necesară în scopul interesului legitim urmărit de operator sau de o parte terță, astfel cum se menționează la articolul 6 alineatul (1) litera (f) din regulamentul respectiv, precum și în contextul prelucrării datelor cu caracter personal care este necesară pentru îndeplinirea unei obligații legale care îi revine operatorului, necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul, astfel cum se menționează la articolul 6 alineatul (1) literele (c) și, respectiv, (e) din regulamentul respectiv.

([13]) 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).

(35) Pentru a menține un nivel ridicat de reziliență operațională digitală pentru întregul sector financiar și, în același timp, pentru a ține pasul cu evoluțiile tehnologice, prezentul regulament ar trebui să abordeze riscurile care decurg din toate tipurile de servicii TIC. În acest scop, definiția serviciilor TIC în contextul prezentului regulament ar trebui înțeleasă în sens larg, incluzând serviciile digitale și de date furnizate în mod continuu prin intermediul sistemelor TIC unuia sau mai multor utilizatori interni sau externi. Această definiție ar trebui, de exemplu, să includă așa-numitele servicii „over the top", care se încadrează în categoria serviciilor de comunicații electronice. Definiția ar trebui să excludă numai categoria limitată de servicii tradiționale de telefonie analogică care pot fi calificate drept servicii ale rețelei publice comutate de telefonie (PSTN), servicii care utilizează linii terestre, servicii de telefonie istorice (POTS) sau servicii de linii telefonice fixe.

(36) 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 lor **și** al profilului general de risc. Ca principiu general, atunci când se distribuie resurse și capacități către punerea în aplicare a cadrului de gestionare a riscurilor TIC, entitățile financiare ar trebui să asigure un echilibru corespunzător între nevoile lor în materie de TIC și dimensiunea și profilul lor general de risc, precum și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor, în timp ce autoritățile competente ar trebui să continue să evalueze și să revizuiască abordarea acestei distribuiri.

(37) Prestatorii de servicii de informare cu privire la conturi, menționați la articolul 33 alineatul (1) din Directiva (UE) 2015/2366, sunt incluși în mod explicit în domeniul de aplicare al prezentului regulament, ținând seama de natura specifică a activităților lor și de riscurile care decurg din acestea. În plus, instituțiile emitente de monedă electronică și instituțiile de plată care sunt exceptate în temeiul articolului 9 alineatul (1) din Directiva 2009/110/CE a Parlamentului European și a Consiliului ([14]) și al articolului 32 alineatul (1) din Directiva (UE) 2015/2366 sunt incluse în domeniul de aplicare al prezentului regulament chiar dacă nu au fost autorizate, în conformitate cu Directiva 2009/110/CE, să emită monedă electronică sau dacă nu au fost autorizate, în conformitate cu Directiva (UE) 2015/2366, să furnizeze și să presteze servicii de plată. Cu toate acestea, oficiile poștale care efectuează operațiuni de virament, menționate la articolul 2 alineatul (5) punctul 3 din Directiva 2013/36/UE a Parlamentului European și a Consiliului ([15]), sunt excluse din domeniul de aplicare al prezentului regulament. Autoritatea competentă pentru instituțiile de plată exceptate în temeiul Directivei (UE) 2015/2366, instituțiile emitente de monedă electronică exceptate în temeiul Directivei 2009/110/CE și prestatorii de servicii de informare cu privire la conturi menționați la articolul 33 alineatul (1) din Directiva (UE) 2015/2366 ar trebui să fie autoritatea competentă desemnată în conformitate cu articolul 22 din Directiva (UE) 2015/2366.

(38) Întrucât entitățile financiare mai mari s-ar putea bucura de resurse mai ample și pot 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 modelul celor trei linii de apărare sau pentru a institui un model intern de gestionare și control al riscurilor și pentru a supune cadrul lor de gestionare a riscurilor TIC auditurilor interne.

(39) Unele entități financiare beneficiază de derogări sau fac obiectul unui cadru de reglementare foarte puțin strict în temeiul legislației sectoriale relevante a Uniunii. Printre aceste entități financiare se numără administratorii de fonduri de investiții alternative menționați la articolul 3 alineatul (2) din Directiva 2011/61/UE a Parlamentului European și a Consiliului ([16]), întreprinderile de asigurare și de reasigurare menționate la articolul 4 din Directiva 2009/138/CE a Parlamentului European și a Consiliului ([17]) și instituțiile pentru furnizarea de pensii ocupaționale

([14]) 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).

([15]) Directiva 2013/36/UE a Parlamentului European și a Consiliului din 26 iunie 2013 cu privire la accesul la activitatea instituțiilor de credit și supravegherea prudențială a instituțiilor de credit, de modificare a Directivei 2002/87/CE și de abrogare a Directivelor 2006/48/CE și 2006/49/CE (JO L 176, 27.6.2013, p. 338).

([16]) Directiva 2011/61/UE a Parlamentului European și a Consiliului din 8 iunie 2011 privind administratorii fondurilor de investiții alternative și de modificare a Directivelor 2003/41/CE și 2009/65/CE și a Regulamentelor (CE) nr. 1060/2009 și (UE) nr. 1095/2010 (JO L 174, 1.7.2011, p. 1).

([17]) Directiva 2009/138/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 privind accesul la activitate și desfășurarea activității de asigurare și de reasigurare (Solvabilitate II), (JO L 335, 17.12.2009, p. 1).

care gestionează sisteme de pensii care împreună nu au mai mult de 15 membri în total. Având în vedere aceste derogări, includerea unor astfel de entități financiare în domeniul de aplicare al prezentului regulament ar fi disproporționată. În plus, prezentul regulament recunoaște particularitățile structurii pieței de intermediere de asigurări, astfel încât intermediarii de asigurări, intermediarii de reasigurări și intermediarii de asigurări auxiliare care pot fi calificați drept microîntreprinderi sau drept întreprinderi mici sau mijlocii nu ar trebui să facă obiectul prezentului regulament.

(40) Întrucât entitățile menționate la articolul 2 alineatul (5) punctele 4-23 din Directiva 2013/36/UE sunt excluse din domeniul de aplicare al directivei respective, statele membre ar trebui, prin urmare, să poată alege să excepteze de la aplicarea prezentului regulament astfel de entități situate pe teritoriile lor respective.

(41) În mod similar, pentru a alinia prezentul regulament la domeniul de aplicare al Directivei 2014/65/UE a Parlamentului European și a Consiliului ([18]), este, de asemenea, oportun să se excludă din domeniul de aplicare al prezentului regulament persoanele fizice și juridice menționate la articolele 2 și 3 din directiva respectivă care sunt autorizate să presteze servicii de investiții fără a trebui să obțină o autorizație în temeiul Directivei 2014/65/UE. Cu toate acestea, articolul 2 din Directiva 2014/65/UE exclude, de asemenea, din domeniul de aplicare al directivei respective entități care pot fi calificate drept entități financiare în sensul prezentului regulament, cum ar fi depozitarii centrali de titluri de valoare, organismele de plasament colectiv sau întreprinderile de asigurare și de reasigurare. Excluderea din domeniul de aplicare al prezentului regulament a persoanelor și entităților menționate la articolele 2 și 3 din directiva respectivă nu ar trebui să includă depozitarii centrali de titluri de valoare, organismele de plasament colectiv sau întreprinderile de asigurare și de reasigurare.

(42) În temeiul legislației sectoriale a Uniunii, unele entități financiare fac obiectul unor cerințe sau exceptări mai puțin stricte din motive legate de dimensiunea lor sau de serviciile pe care le furnizează. Categoria respectivă de entități financiare include firmele de investiții mici și neinterconectate, instituțiile mici pentru furnizarea de pensii ocupaționale care pot fi excluse din domeniul de aplicare al Directivei (UE) 2016/2341 în condițiile prevăzute la articolul 5 din directiva respectivă de către statul membru în cauză și care gestionează sisteme de pensii care împreună nu au mai mult de 100 de membri în total, precum și instituțiile exceptate în temeiul Directivei 2013/36/UE. Prin urmare, în conformitate cu principiul proporționalității și pentru a păstra spiritul legislației sectoriale a Uniunii, este, de asemenea, oportun ca aceste entități financiare să facă obiectul unui cadru simplificat de gestionare a riscurilor TIC în temeiul prezentului regulament. Caracterul proporțional al cadrului de gestionare a riscurilor TIC care acoperă aceste entități financiare nu ar trebui să fie modificat de standardele tehnice de reglementare care urmează să fie elaborate de AES. În plus, în conformitate cu principiul proporționalității, este oportun, de asemenea, ca instituțiile de plată menționate la articolul 32 alineatul (1) din Directiva (UE) 2015/2366 și instituțiile emitente de monedă electronică menționate la articolul 9 din Directiva 2009/110/CE care sunt exceptate în conformitate cu dreptul intern de transpunere a respectivelor acte juridice ale Uniunii să facă obiectul unui cadru simplificat de gestionare a riscurilor TIC în temeiul prezentului regulament, în timp ce instituțiile de plată și instituțiile emitente de monedă electronică care nu au fost exceptate în conformitate cu dreptul intern de transpunere a legislației sectoriale a Uniunii ar trebui să respecte cadrul general stabilit de prezentul regulament.

(43) În mod similar, entitățile financiare care pot fi calificate drept microîntreprinderi sau care fac obiectul cadrului simplificat de gestionare a riscurilor TIC în temeiul prezentului regulament nu ar trebui să fie obligate să stabilească un rol de monitorizare a acordurilor încheiate cu furnizori terți de servicii TIC cu privire la utilizarea serviciilor TIC; sau să desemneze un membru al conducerii de nivel superior drept responsabil de supravegherea expunerii la risc aferente și a documentației relevante; să atribuie unei funcții de control responsabilitatea pentru gestionarea și supravegherea riscurilor TIC și să asigure un nivel adecvat de independență acestei funcții de control pentru a evita conflictele de interese; să documenteze și să revizuiască cel puțin o dată pe an cadrul de gestionare a riscurilor TIC; să asigure realizarea unui audit intern periodic cu privire la cadrul de gestionare a riscurilor TIC; să efectueze evaluări aprofundate în urma unor schimbări majore în infrastructurile și procesele lor de rețea și ale sistemului informatic; să efectueze în mod regulat analize de risc privind sistemele TIC moștenite; să supună punerea în aplicare a planurilor de răspuns și de recuperare în domeniul TIC unor audituri interne independente; să aibă o funcție de gestionare a crizelor, să extindă testarea planurilor privind continuarea activității și a planurilor de răspuns și de recuperare pentru a integra în aceasta scenariile de transfer între infrastructura TIC primară și instalațiile redundante; să raporteze autorităților competente, la cererea acestora, o estimare a costurilor și

([18]) Directiva 2014/65/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Directivei 2002/92/CE și a Directivei 2011/61/UE (JO L 173, 12.6.2014, p. 349).

pierderilor anuale agregate cauzate de incidentele majore legate de TIC; să mențină capacități TIC redundante; să comunice autorităților naționale competente modificările puse în aplicare în urma verificărilor ulterioare incidentelor legate de TIC; să monitorizeze în permanență evoluțiile tehnologice relevante, să instituie un program cuprinzător de testare a rezilienței operaționale digitale ca parte integrantă a cadrului de gestionare a riscurilor TIC prevăzut în prezentul regulament sau să adopte și să revizuiască periodic o strategie privind riscurile TIC generate de părți terțe. În plus, microîntreprinderilor ar trebui să li se solicite să evalueze necesitatea menținerii unor astfel de capacități TIC redundante numai pe baza profilului lor de risc. Microîntreprinderile ar trebui să beneficieze de un regim mai flexibil în ceea ce privește programele de testare a rezilienței operaționale digitale. Atunci când analizează tipul și frecvența testelor care urmează să fie efectuate, acestea ar trebui să asigure un echilibru corespunzător între obiectivul de a menține un nivel ridicat de reziliență operațională digitală, resursele disponibile și profilul general de risc al acestora. Microîntreprinderile și entitățile financiare care fac obiectul cadrului simplificat de gestionare a riscurilor TIC în temeiul prezentului regulament ar trebui să fie exceptate de la obligația de a efectua testări avansate ale instrumentelor, sistemelor și proceselor TIC pe baza testelor de penetrare bazate pe amenințări (TLPT), întrucât numai entitățile financiare care îndeplinesc criteriile stabilite în prezentul regulament ar trebui să fie obligate să efectueze astfel de teste. Având în vedere capacitățile lor limitate, microîntreprinderile ar trebui să poată conveni cu furnizorul terț de servicii TIC să delege drepturile de acces, inspecție și audit ale entității financiare unei părți terțe independente, care urmează să fie desemnată de furnizorul terț de servicii TIC, cu condiția ca entitatea financiară să poată solicita în orice moment toate informațiile și garanțiile relevante cu privire la performanța furnizorului terț de servicii TIC de la partea terță independentă respectivă.

(44) Întrucât numai acele entități financiare care au fost identificate 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 suportate de către un procent mic de entități financiare.

(45) 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, organele de conducere ale entităților financiare 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 operațională digitală. Abordarea care urmează să fie adoptată de organele 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 mai importantă 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.

(46) În plus, principiul responsabilității depline și finale a organului de conducere pentru gestionarea riscurilor TIC ale entității financiare este în strânsă legătură cu necesitatea de a asigura un nivel de investiții legate de TIC și un buget general pentru entitatea financiară care i-ar permite acesteia să atingă un nivel ridicat de reziliență operațională digitală.

(47) Inspirat de bunele practici, de orientările, recomandările și abordările relevante emise la nivel internațional, național și sectorial privind gestionarea riscului cibernetic, prezentul regulament promovează un set de principii care facilitează structura globală a gestionării riscurilor TIC. Prin urmare, atât timp cât principalele capacități pe care entitățile financiare le instituie abordează diversele funcții în gestionarea riscurilor TIC (identificare, protecție și prevenire, detectare, răspuns și recuperare, învățare și evoluție și comunicare) stabilite în prezentul regulament, entitățile financiare ar trebui să aibă în continuare libertatea de a utiliza modele de gestionare a riscurilor TIC diferit formulate sau clasificate.

(48) 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 capabile nu numai de a garanta prelucrarea datelor necesară pentru executarea serviciilor lor, ci și de a asigura o reziliență tehnologică suficientă care să le permită să trateze în mod adecvat nevoile de prelucrare suplimentare cauzate de condiții de criză a pieței sau de alte situații adverse.

(49) Sunt necesare planuri eficace de continuitate a activității și recuperare 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 acțiunilor de recuperare în conformitate cu politicile lor privind copiile de rezervă. Cu toate acestea, o astfel de reluare a activității nu ar trebui în niciun caz să pună în pericol integritatea și securitatea rețelelor și a sistemelor informatice sau disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor.

(50) Deși prezentul regulament permite entităților financiare să-și stabilească obiectivele cu privire la intervalele de timp și momentele de la care se pot recupera datele în urma unei întreruperi și intervalele maxime de recuperare în urma unei întreruperi, într-un mod flexibil și, prin urmare, să stabilească astfel de obiective ținând seama pe deplin de natura și de importanța funcțiilor relevante și de orice nevoi funcționale specifice, o evaluare a impactului global potențial asupra eficienței pieței ar trebui să fie obligatorie atunci când entitățile financiare stabilesc astfel de obiective.

(51) Propagatorii atacurilor cibernetice tind să urmărească câștiguri financiare direct la sursă, expunând astfel entitățile financiare la consecințe semnificative. Pentru a preveni pierderea integrității sistemelor TIC sau indisponibilitatea acestora și, prin urmare, pentru a evita încălcarea securității datelor și deteriorarea infrastructurii fizice TIC, raportarea incidentelor majore legate de TIC de către entitățile financiare ar trebui să fie îmbunătățită și raționalizată în mod semnificativ. Raportarea incidentelor legate de TIC ar trebui armonizată prin introducerea unei cerințe pentru toate entitățile financiare de a raporta direct autorităților lor competente relevante. În cazul în care o entitate financiară face obiectul supravegherii de către mai multe autorități naționale competente, statele membre ar trebui să desemneze o singură autoritate competentă ca destinatar al unei astfel de raportări. Instituțiile de credit clasificate drept semnificative în conformitate cu articolul 6 alineatul (4) din Regulamentul (UE) nr. 1024/2013 al Consiliului ([19]) ar trebui să transmită aceste raportări autorităților naționale competente, care ar trebui să transmită ulterior raportul Băncii Centrale Europene (BCE).

(52) Raportarea directă ar trebui să permită autorităților de supraveghere financiară să aibă acces imediat la informații cu privire la incidentele majore legate de TIC. Autoritățile de supraveghere financiară ar trebui, la rândul lor, să transmită detaliile incidentelor majore legate de TIC autorităților nefinanciare publice [cum ar fi autoritățile competente și punctele unice de contact în temeiul Directivei (UE) 2022/2555, autoritățile naționale de protecție a datelor și autoritățile de aplicare a legii în cazul incidentelor majore legate de TIC de natură penală] pentru a spori gradul de conștientizare a acestor autorități cu privire la astfel de incidente și, în cazul echipelor CSIRT, pentru a facilita asistența promptă care poate fi acordată entităților financiare, după caz. În plus, statele membre ar trebui să poată stabili că entitățile financiare sunt cele care ar trebui să furnizeze astfel de informații autorităților publice din afara domeniului serviciilor financiare. Respectivele fluxuri de informații ar trebui să le permită entităților financiare să beneficieze rapid de orice contribuție tehnică relevantă, de consiliere cu privire la măsurile corective și de măsurile subsecvente luate de aceste autorități. Informațiile privind incidentele majore legate de TIC ar trebui canalizate reciproc: autoritățile de supraveghere financiară ar trebui să ofere entității financiare tot feedbackul sau toate orientările necesare, în timp ce AES ar trebui să partajeze date anonimizate privind amenințările cibernetice și vulnerabilitățile legate de un incident, pentru a contribui la o apărare colectivă mai amplă.

(53) Deși toate entitățile financiare ar trebui să aibă obligația de a efectua raportarea incidentelor, nu se preconizează că această cerință le va afecta pe toate în aceeași măsură. Într-adevăr, pragurile de semnificație relevante, precum și termenele de raportare ar trebui să fie ajustate în mod corespunzător, în contextul actelor delegate bazate pe standardele tehnice de reglementare care urmează să fie elaborate de AES, pentru a acoperi numai incidentele majore legate de TIC. În plus, la stabilirea termenelor pentru obligațiile de raportare ar trebui să se țină seama de particularitățile entităților financiare.

(54) Prezentul regulament ar trebui să impună instituțiilor de credit, instituțiilor de plată, prestatorilor de servicii de informare cu privire la conturi și instituțiilor emitente de monedă electronică să raporteze toate incidentele operaționale sau de securitate legate de plăți – raportate anterior în temeiul Directivei (UE) 2015/2366 – indiferent de natura incidentului, legată sau nu de TIC.

([19]) 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).

(55) AES ar trebui să aibă sarcina de a evalua fezabilitatea și condițiile unei posibile centralizări a rapoartelor privind incidentele legate de TIC la nivelul Uniunii. O astfel de centralizare ar putea consta într-o platformă unică a UE pentru raportarea incidentelor majore legate de TIC, care fie să primească direct rapoartele relevante și să notifice automat autoritățile naționale competente, fie doar să centralizeze rapoartele relevante transmise de autoritățile naționale competente, îndeplinind astfel un rol de coordonare. AES ar trebui să aibă sarcina de a pregăti, în consultare cu BCE și ENISA, un raport comun în care să analizeze fezabilitatea instituirii unei platforme unice la nivelul UE.

(56) Pentru a atinge un nivel ridicat de reziliență operațională digitală și în conformitate atât cu standardele internaționale relevante (de exemplu, elementele fundamentale ale G7 pentru testele de penetrare bazate pe amenințări), cât și cu cadrele aplicate în Uniune, cum ar fi TIBER-UE, entitățile financiare ar trebui să își testeze periodic sistemele TIC și personalul care are responsabilități legate de TIC în ceea ce privește eficacitatea capacităților lor de prevenire, detectare, răspuns și recuperare, pentru a descoperi și a aborda potențialele vulnerabilități TIC. Pentru a reflecta diferențele existente între diferitele subsectoare financiare și în interiorul acestora în ceea ce privește nivelul de pregătire în materie de securitate cibernetică al entităților financiare, testarea ar trebui să includă o gamă largă de instrumente și acțiuni, de la evaluarea cerințelor de bază (de exemplu, evaluări și examinări ale vulnerabilităților, analize ale surselor deschise, evaluări ale securității rețelelor, analize ale lacunelor, verificări ale securității fizice, chestionare și soluții de analiză de tip software, evaluări ale codului sursă unde este posibil, teste bazate pe scenarii, teste de compatibilitate, teste de performanță sau teste de la un capăt la altul) până la testări mai avansate cu ajutorul TLPT. Astfel de testări mai avansate ar trebui să fie obligatorii numai pentru entitățile financiare care sunt suficient de mature din perspectiva TIC pentru a le efectua în mod rezonabil. Prin urmare, testarea rezilienței operaționale digitale impusă prin prezentul regulament ar trebui să fie mai riguroasă pentru entitățile financiare care îndeplinesc criteriile stabilite în prezentul regulament (de exemplu, instituțiile de credit mari, sistemice și cu o TIC matură, bursele de valori, depozitarii centrali de titluri de valoare și contrapărțile centrale) decât pentru alte entități financiare. În același timp, testarea rezilienței operaționale digitale prin intermediul TLPT ar trebui să fie mai relevantă pentru entitățile financiare care operează în subsectoare ale serviciilor financiare esențiale și care joacă un rol sistemic (de exemplu, plăți, servicii bancare și compensări și decontări) și mai puțin relevantă pentru alte subsectoare (de exemplu, administratorii de active și agențiile de rating de credit).

(57) Entitățile financiare implicate în activități transfrontaliere și 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, TLPT) în statul membru de origine, care ar trebui să includă infrastructurile TIC din toate jurisdicțiile în care grupul financiar transfrontalier își desfășoară activitatea pe teritoriul Uniunii, permițând astfel acestor grupuri financiare transfrontaliere să suporte costurile de testare legate de TIC într-o singură jurisdicție.

(58) Pentru a fructifica expertiza deja dobândită de anumite autorități competente, în special în ceea ce privește punerea în aplicare a cadrului TIBER-UE, prezentul regulament ar trebui să permită statelor membre să desemneze o singură autoritate publică responsabilă în sectorul financiar, la nivel național, pentru toate aspectele legate de TLPT, sau autorităților competente să delege, în absența unei astfel de desemnări, exercitarea sarcinilor legate de TLPT unei alte autorități financiare naționale competente.

(59) Întrucât prezentul regulament nu impune entităților financiare să acopere toate funcțiile critice sau importante în cadrul unui singur test de penetrare bazat pe amenințări, entitățile financiare ar trebui să aibă libertatea de a stabili care funcții critice sau importante și câte astfel de funcții ar trebui incluse în sfera unui astfel de test.

(60) Testarea grupată în sensul prezentului regulament – care implică participarea mai multor entități financiare la un TLPT și pentru care un furnizor terț de servicii TIC poate încheia în mod direct acorduri contractuale cu o entitate externă de testare – ar trebui să fie permisă numai în cazul în care se preconizează în mod rezonabil că vor fi afectate în mod negativ calitatea sau securitatea serviciilor furnizate de furnizorul terț de servicii TIC clienților care sunt entități care nu intră în domeniul de aplicare al prezentului regulament, sau confidențialitatea datelor referitoare la astfel de servicii. Testarea grupată ar trebui, de asemenea, să facă obiectul unor garanții (conducerea de către o entitate financiară desemnată, calibrarea numărului de entități financiare participante) pentru a asigura un exercițiu de testare riguros pentru entitățile financiare implicate care îndeplinesc obiectivele TLPT în temeiul prezentului regulament.

(61) Pentru a profita de resursele interne disponibile la nivel corporativ, prezentul regulament ar trebui să permită utilizarea unor entități interne de testare în scopul efectuării TLPT, cu condiția să existe aprobarea autorității de supraveghere, să nu existe conflicte de interese și să existe o alternare periodică între utilizarea entităților interne și a celor externe de testare (la fiecare trei teste), solicitând, în același timp, ca furnizorul de informații privind amenințările din TLPT să fie întotdeauna extern entității financiare. Responsabilitatea pentru desfășurarea TLPT ar trebui să revină în totalitate entității financiare. Atestările furnizate de autorități ar trebui să fie exclusiv în scopul recunoașterii reciproce și nu ar trebui să împiedice nicio acțiune ulterioară necesară pentru a aborda riscurile TIC la care este expusă entitatea financiară și nici nu ar trebui să fie considerate drept o validare de către autoritățile de supraveghere a capacităților unei entități financiare de gestionare și atenuare a riscurilor TIC.

(62) Pentru a asigura o monitorizare solidă a riscurilor TIC generate de părți terțe în sectorul financiar, este necesar să se stabilească un set de norme bazate pe principii care să ghideze entitățile financiare atunci când monitorizează riscurile care apar în contextul funcțiilor externalizate către furnizorii terți de servicii TIC, în special cu privire la serviciile TIC care sprijină funcții critice sau importante, precum și, la un nivel mai general, în contextul tuturor dependențelor față de furnizorii terți de servicii TIC.

(63) Pentru a aborda complexitatea diferitelor surse de riscuri TIC, ținând seama, în același timp, de multitudinea și diversitatea furnizorilor de soluții tehnologice care permit furnizarea fără probleme a serviciilor financiare, prezentul regulament ar trebui să acopere o gamă largă de furnizori terți de servicii TIC, inclusiv furnizori de servicii de cloud computing, software, servicii de analiză a datelor și furnizori de servicii de centre de date. În mod similar, întrucât entitățile financiare ar trebui să identifice și să gestioneze în mod eficace și coerent toate tipurile de riscuri, inclusiv în contextul serviciilor TIC achiziționate în cadrul unui grup financiar, ar trebui să se clarifice faptul că întreprinderile care fac parte dintr-un grup financiar și furnizează servicii TIC în principal societății-mamă sau filialelor ori sucursalelor societății-mamă a acestora, precum și entitățile financiare care furnizează servicii TIC altor entități financiare ar trebui, de asemenea, să fie considerate furnizori terți de servicii TIC în temeiul prezentului regulament. În cele din urmă, având în vedere evoluția pieței serviciilor de plată, care devine din ce în ce mai dependentă de soluții tehnice complexe și având în vedere tipurile emergente de servicii de plată și soluțiile legate de plăți, participanții la ecosistemul serviciilor de plată, la furnizarea de activități de procesare a plăților sau la exploatarea infrastructurilor de plată ar trebui, de asemenea, să fie considerați drept furnizori terți de servicii TIC în temeiul prezentului regulament, cu excepția băncilor centrale atunci când operează sisteme de plată sau de decontare a titlurilor de valoare, precum și a autorităților publice atunci când furnizează servicii legate de TIC în contextul îndeplinirii funcțiilor statului.

(64) O entitate financiară ar trebui să rămână în orice moment pe deplin responsabilă de respectarea obligațiilor sale prevăzute în prezentul regulament. Entitățile financiare ar trebui să aplice o abordare proporțională în ceea ce privește monitorizarea riscurilor care apar la nivelul furnizorilor terți de servicii TIC, ținând seama în mod corespunzător de natura, amploarea, complexitatea și importanța dependențelor lor legate de TIC, de caracterul critic sau de importanța serviciilor, proceselor sau funcțiilor care fac obiectul acordurilor contractuale și, în cele din urmă, în baza unei evaluări atente a oricărui impact potențial asupra continuității și calității serviciilor financiare la nivel individual și la nivel de grup, după caz.

(65) 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 privind riscurile TIC generate de părți terțe, bazate pe o verificare continuă a tuturor acestor dependențe față de furnizorii terți de servicii TIC. Pentru a spori gradul de conștientizare în materie de supraveghere cu privire la dependențele față de furnizorii terți de servicii TIC și în vederea sprijinirii suplimentare a activității în contextul cadrului de supraveghere instituit prin prezentul regulament, toate entitățile financiare ar trebui să aibă obligația de a menține un registru de informații cu privire la toate acordurile contractuale privind utilizarea serviciilor TIC oferite de furnizori terți de servicii TIC. Autoritățile de supraveghere financiară ar trebui să fie în măsură să solicite registrul complet sau să solicite secțiuni specifice din acesta și, astfel, să obțină informații esențiale pentru a înțelege mai bine dependențele în materie de TIC ale entităților financiare.

(66) O analiză precontractuală aprofundată ar trebui să stea la baza încheierii formale a acordurilor contractuale, în special prin axarea pe elemente precum caracterul critic sau importanța serviciilor sprijinite de contractul TIC avut în vedere, aprobările necesare din partea autorităților de supraveghere sau alte condiții, posibilul risc de concentrare implicat, precum și aplicând toate diligențele necesare în procesul de selecție și evaluare a furnizorilor terți de servicii TIC și prin evaluarea potențialelor conflicte de interese. În ceea ce privește acordurile contractuale privind funcțiile critice sau importante, entitățile financiare ar trebui să ia în considerare utilizarea de către furnizorii terți de servicii TIC a celor mai recente și mai înalte standarde de securitate a informațiilor. Încetarea acordurilor contractuale ar putea fi determinată de cel puțin o serie de circumstanțe care indică deficiențe la nivelul furnizorului terț de servicii

TIC, în special încălcări semnificative ale legislației sau ale clauzelor contractuale, circumstanțe care indică o posibilă modificare a îndeplinirii funcțiilor prevăzute în acordurile contractuale, dovezi ale deficiențelor furnizorului terț de servicii TIC în gestionarea globală a riscurilor TIC sau circumstanțe care indică incapacitatea autorității competente relevante de a supraveghea în mod eficace entitatea financiară.

(67) Pentru a aborda impactul sistemic al riscului de concentrare a serviciilor TIC furnizate de către părți terțe, prezentul regulament promovează o soluție echilibrată prin adoptarea unei abordări flexibile și progresive cu privire la un astfel de risc de concentrare, deoarece impunerea unor plafoane rigide sau limitări stricte ar putea împiedica desfășurarea activității comerciale și ar putea restrânge libertatea contractuală. Entitățile financiare ar trebui să evalueze în detaliu acordurile contractuale preconizate pentru a identifica probabilitatea apariției unui astfel de risc, inclusiv prin intermediul unor analize aprofundate ale acordurilor de subcontractare, 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 de a menține libertatea contractuală și cea de a garanta stabilitatea financiară, nu se consideră adecvat să se stabilească norme privind plafoane și limite stricte pentru expunerile la furnizorii terți de servicii TIC. În ceea ce privește cadrul de supraveghere, un supraveghetor principal numit în temeiul prezentului regulament ar trebui, în ceea ce privește furnizorii terți esențiali de servicii TIC, să acorde o atenție deosebită înțelegerii depline a amplorii interdependențelor și descoperirii cazurilor specifice în care un grad ridicat de concentrare a furnizorilor terți esențiali de servicii TIC din Uniune este susceptibil să exercite o presiune asupra stabilității și integrității sistemului financiar al Uniunii și să mențină un dialog cu furnizorii terți esențiali de servicii TIC, în cazurile în care acest risc specific este identificat.

(68) Pentru a evalua și monitoriza în mod regulat capacitatea unui furnizor terț de servicii TIC de a furniza servicii în condiții de siguranță unei entități financiare fără efecte negative asupra rezilienței operaționale digitale a unei entități financiare, ar trebui armonizate mai multe elemente contractuale esențiale cu furnizorii terți de servicii TIC. O astfel de armonizare ar trebui să acopere domeniile minime care sunt esențiale pentru a permite o monitorizare completă de către entitatea financiară a riscurilor care ar putea fi generate de furnizorul terț de servicii TIC, din perspectiva necesității unei entități financiare de a-și asigura reziliența digitală, deoarece aceasta depinde în mare măsură de stabilitatea, funcționalitatea, disponibilitatea și securitatea serviciilor TIC primite.

(69) La renegocierea acordurilor contractuale pentru a urmări alinierea la cerințele prezentului regulament, entitățile financiare și furnizorii terți de servicii TIC ar trebui să se asigure că acoperă principalele dispoziții contractuale prevăzute în prezentul regulament.

(70) Definiția „funcției critice sau importante” prevăzută în prezentul regulament ar trebui să includă „funcțiile critice” astfel cum sunt definite la articolul 2 alineatul (1) punctul 35 din Directiva 2014/59/UE a Parlamentului European și a Consiliului ([20]). În consecință, funcțiile considerate critice în temeiul Directivei 2014/59/UE sunt incluse în definiția funcțiilor critice în sensul prezentului regulament.

(71) Independent de caracterul critic sau de importanța funcției sprijinite de serviciile TIC, acordurile contractuale ar trebui, în special, să prevadă specificații cu privire la descrierile complete ale funcțiilor și serviciilor, a locurilor în care sunt furnizate astfel de funcții și în care urmează să fie prelucrate datele, precum și o indicare a descrierilor la nivelul serviciilor. Alte elemente esențiale pentru a permite unei entități financiare să monitorizeze riscurile TIC generate de părți terțe sunt: dispozițiile contractuale care specifică modul în care accesibilitatea, disponibilitatea, integritatea, securitatea și protecția datelor cu caracter personal sunt asigurate de furnizorul terț de servicii TIC, dispozițiile care stabilesc garanțiile relevante pentru a permite accesul, recuperarea și restituirea datelor în caz de insolvență, rezoluție sau întrerupere a operațiunilor comerciale ale furnizorului terț de servicii TIC, precum și dispozițiile care impun furnizorului terț de servicii TIC să ofere asistență în cazul unor incidente TIC în legătură cu serviciile furnizate, fără costuri suplimentare sau la un cost stabilit ex ante; dispozițiile privind obligația furnizorului

([20]) Directiva 2014/59/UE a Parlamentului European și a Consiliului din 15 mai 2014 de instituire a unui cadru pentru redresarea și rezoluția instituțiilor de credit și a firmelor de investiții și de modificare a Directivei 82/891/CEE a Consiliului și a Directivelor 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE și 2013/36/UE și a Regulamentelor (UE) nr. 1093/2010 și (UE) nr. 648/2012 ale Parlamentului European și ale Consiliului (JO L 173, 12.6.2014, p. 190).

terț de servicii TIC de a coopera pe deplin cu autoritățile competente și cu autoritățile de rezoluție ale entității financiare și dispozițiile privind drepturile de încetare și perioade minime de preaviz aferente încetării acordurilor contractuale, în conformitate cu așteptările autorităților competente și ale autorităților de rezoluție.

(72) În plus față de aceste dispoziții contractuale și pentru a se asigura că entitățile financiare păstrează controlul deplin asupra tuturor evoluțiilor care au loc la nivelul terților și care le pot afecta securitatea TIC, contractele pentru furnizarea de servicii TIC care sprijină funcții critice sau importante ar trebui, de asemenea, să prevadă următoarele: specificarea descrierilor complete la nivelul serviciilor, cu obiective de performanță cantitative și calitative precise, pentru a permite, fără întârzieri nejustificate, luarea de măsuri corective adecvate atunci când nivelurile convenite ale serviciilor nu sunt atinse; perioadele de preaviz și obligațiile de raportare relevante ale furnizorului terț de servicii TIC în cazul unor evoluții cu un potențial impact semnificativ asupra capacității furnizorului terț de servicii TIC de a furniza în mod eficace serviciile TIC respective; o cerință impusă furnizorului terț de servicii TIC de a pune în aplicare și de a testa planuri pentru situații neprevăzute și de a dispune de măsuri, instrumente și politici de securitate TIC care să permită furnizarea în condiții de siguranță a serviciilor, precum și de a participa și de a coopera pe deplin la TLPT efectuat de entitatea financiară.

(73) Contractele pentru furnizarea de servicii TIC care sprijină funcții critice sau importante ar trebui să conțină, de asemenea, dispoziții care să permită drepturile de acces, de inspecție și de audit exercitate de entitatea financiară sau de o parte terță desemnată, precum și dreptul de a produce copii ca instrumente esențiale pentru monitorizarea continuă de către entitățile financiare a performanței furnizorului terț de servicii TIC, alături de deplina cooperare a furnizorului de servicii în timpul inspecțiilor. În mod similar, autoritatea competentă a entității financiare ar trebui să dispună de dreptul, pe baza unor preavize, de a inspecta și a audita furnizorul terț de servicii TIC, sub rezerva protecției informațiilor confidențiale.

(74) Astfel de acorduri contractuale ar trebui, de asemenea, să prevadă strategii de ieșire specifice pentru a asigura, în special, perioade de tranziție obligatorii în cursul cărora furnizorii terți de servicii TIC ar trebui să continue să furnizeze serviciile relevante în vederea reducerii riscului de perturbări la nivelul entității financiare sau pentru a permite acesteia din urmă să treacă efectiv la utilizarea altor furnizori terți de servicii TIC sau, alternativ, să treacă la utilizarea de soluții dezvoltate pe plan intern, în concordanță cu complexitatea serviciului TIC furnizat. În plus, entitățile financiare care intră în domeniul de aplicare al Directivei 2014/59/UE ar trebui să se asigure că contractele relevante pentru servicii TIC sunt solide și pe deplin executorii în cazul rezoluției respectivelor entități financiare. Prin urmare, în conformitate cu așteptările autorităților de rezoluție, entitățile financiare respective ar trebui să se asigure că contractele relevante pentru serviciile TIC sunt reziliente în ceea ce privește rezoluția. Atât timp cât își îndeplinesc în continuare obligațiile de plată, entitățile financiare respective ar trebui să se asigure, printre alte cerințe, că contractele relevante pentru servicii TIC conțin clauze de neîncetare, de nesuspendare și de nemodificare din motive de restructurare sau de rezoluție.

(75) În plus, utilizarea voluntară a clauzelor contractuale standard elaborate de autoritățile publice sau de instituțiile Uniunii, în special utilizarea clauzelor contractuale elaborate de Comisie pentru serviciile de cloud computing ar putea oferi un confort suplimentar entităților financiare și furnizorilor lor terți de servicii TIC, prin creșterea nivelului lor de securitate juridică cu privire la utilizarea serviciilor de cloud computing în sectorul financiar, în deplină conformitate cu cerințele și așteptările prevăzute în dreptul Uniunii privind serviciile financiare. Elaborarea unor clauze contractuale standard se bazează pe măsurile deja prevăzute în Planul de acțiune privind Fintech din 2018, care a anunțat intenția Comisiei de a încuraja și de a facilita elaborarea unor clauze contractuale standard pentru utilizarea externalizării serviciilor de cloud computing de către entitățile financiare, pe baza eforturilor depuse de părțile interesate transsectoriale în domeniul serviciilor de cloud computing, pe care Comisia le-a facilitat cu ajutorul implicării sectorului financiar.

(76) Cu scopul de a promova convergența și eficiența în ceea ce privește abordările în materie de supraveghere a riscurilor TIC generate de părți terțe în sectorul financiar, precum și de a consolida reziliența operațională digitală a entităților financiare care se bazează pe furnizori terți esențiali de servicii TIC pentru furnizarea serviciilor TIC care sprijină furnizarea de servicii financiare, contribuind astfel la menținerea stabilității sistemului financiar al Uniunii și a integrității pieței interne a serviciilor financiare, furnizorii terți esențiali de servicii TIC ar trebui să facă obiectul unui cadru de supraveghere al Uniunii. Deși instituirea cadrului de supraveghere este justificată de valoarea adăugată a luării de măsuri la nivelul Uniunii și de rolul inerent și particularitățile utilizării serviciilor TIC în furnizarea de

servicii financiare, ar trebui reamintit, în același timp, că această soluție pare adecvată numai în contextul prezentului regulament, care abordează în mod specific reziliența operațională digitală în sectorul financiar. Cu toate acestea, un astfel de cadru de supraveghere nu ar trebui considerat un nou model de supraveghere la nivelul Uniunii în domeniul serviciilor și activităților financiare.

(77) Cadrul de supraveghere ar trebui să se aplice numai furnizorilor terți esențiali de servicii TIC. Prin urmare, ar trebui să existe un mecanism de desemnare care să țină seama de dimensiunea și natura dependenței sectorului financiar de astfel de furnizori terți de servicii TIC. Mecanismul respectiv ar trebui să implice un set de criterii cantitative și calitative pentru a stabili parametrii critici ca bază pentru includerea în cadrul de supraveghere. Pentru a asigura acuratețea acestei evaluări și indiferent de structura corporativă a furnizorului terț de servicii TIC, astfel de criterii ar trebui, în cazul unui furnizor terț de servicii TIC care face parte dintr-un grup mai larg, să ia în considerare întreaga structură de grup a furnizorului terț de servicii TIC. Pe de o parte, furnizorii terți esențiali de servicii TIC care nu sunt desemnați în mod automat în temeiul aplicării criteriilor respective ar trebui să aibă posibilitatea de a opta să fie parte din cadrul de supraveghere în mod voluntar, pe de altă parte, furnizorii terți de servicii TIC care fac deja obiectul cadrelor mecanismului de supraveghere care sprijină îndeplinirea sarcinilor Sistemului European al Băncilor Centrale, astfel cum sunt menționate la articolul 127 alineatul (2) din TFUE, ar trebui să fie exceptați.

(78) În mod similar, entitățile financiare care furnizează servicii TIC altor entități financiare, deși aparțin categoriei furnizorilor terți de servicii TIC în temeiul prezentului regulament, ar trebui, de asemenea, să fie exceptate de la cadrul de supraveghere, deoarece fac deja obiectul mecanismelor de supraveghere instituite prin dreptul relevant al Uniunii privind serviciile financiare. După caz, autoritățile competente ar trebui să țină seama, în contextul activităților lor de supraveghere, de riscurile TIC pe care entitățile financiare care furnizează servicii TIC le prezintă pentru entitățile financiare. De asemenea, având în vedere mecanismele existente de monitorizare a riscurilor la nivel de grup, aceeași derogare ar trebui introdusă pentru furnizorii terți de servicii TIC care furnizează servicii în principal entităților din propriul grup. Furnizorii terți de servicii TIC care furnizează servicii TIC numai într-un stat membru entităților financiare care își desfășoară activitatea numai în statul membru respectiv ar trebui, de asemenea, să fie exceptați de la mecanismul de desemnare din cauza activităților lor limitate și a lipsei impactului transfrontalier.

(79) Transformarea digitală prin care trec serviciile financiare a generat un nivel fără precedent de utilizare a serviciilor TIC și de dependență de acestea. Întrucât a devenit imposibilă furnizarea de servicii financiare fără utilizarea serviciilor de cloud computing, a soluțiilor software și a serviciilor legate de date, ecosistemul financiar al Uniunii a devenit intrinsec codependent de anumite servicii TIC furnizate de furnizorii de servicii TIC. Unii dintre acești furnizori, inovatori în dezvoltarea și aplicarea tehnologiilor bazate pe TIC, joacă un rol semnificativ în furnizarea de servicii financiare sau au devenit integrați în lanțul valoric al serviciilor financiare. Prin urmare, aceștia au devenit esențiali pentru stabilitatea și integritatea sistemului financiar al Uniunii. Această dependență generalizată de serviciile oferite de furnizori terți esențiali de servicii TIC, combinată cu interdependența sistemelor informatice ale diferiților operatori de pe piață, creează un risc direct și potențial grav pentru sistemul de servicii financiare al Uniunii și pentru continuitatea furnizării de servicii financiare în cazul în care furnizorii terți esențiali de servicii TIC ar fi afectați de perturbări operaționale sau de incidente cibernetice majore. Incidentele cibernetice au o capacitate distinctă de a se multiplica și de a se răspândi în întreg sistemul financiar într-un ritm considerabil mai rapid decât alte tipuri de riscuri monitorizate în sectorul financiar și se pot extinde dincolo de sectoare și dincolo de frontierele geografice. Acestea au potențialul de a evolua într-o criză sistemică, în care încrederea în sistemul financiar a fost erodată din cauza perturbării funcțiilor de sprijinire a economiei reale sau a unor pierderi financiare substanțiale, atingând un nivel la care sistemul financiar nu este în măsură să reziste sau care necesită aplicarea unor măsuri de absorbție a șocurilor majore. Pentru a preveni apariția acestor scenarii și, astfel, punerea în pericol a stabilității financiare și a integrității Uniunii, este esențial să se asigure convergența practicilor de supraveghere legate de riscurile TIC generate de părți terțe în domeniul financiar, în special prin noi norme care să permită supravegherea de către Uniune a furnizorilor terți esențiali de servicii TIC.

(80) Cadrul de supraveghere depinde în mare măsură de gradul de colaborare dintre supraveghetorul principal și furnizorul terț esențial de servicii TIC care furnizează entităților financiare servicii care afectează furnizarea de servicii financiare. Supravegherea reușită se bazează, printre altele, pe capacitatea supraveghetorului principal de a efectua în mod eficace misiuni de monitorizare și inspecții pentru a evalua normele, controalele și procesele utilizate de furnizorii terți esențiali de servicii TIC, precum și pe capacitatea de a evalua impactul potențial cumulativ al activităților lor asupra stabilității financiare și a integrității sistemului financiar. În același timp, este esențial ca furnizorii terți esențiali de servicii TIC să urmeze recomandările supraveghetorului principal și să răspundă preocupărilor acestuia. Întrucât o lipsă de cooperare din partea unui furnizor terț esențial de servicii TIC care furnizează servicii care afectează furnizarea de servicii financiare, cum ar fi refuzul de a acorda acces la sediul său sau de a prezenta informații, ar priva, în cele din urmă, supraveghetorul principal de instrumentele sale esențiale de evaluare a riscurilor TIC generate de părți terțe și ar putea avea un impact negativ asupra stabilității financiare și a integrității sistemului financiar, este necesar să se prevadă, de asemenea, un regim de sancționare proporțional.

(81) În acest context, necesitatea ca supraveghetorul principal să impună penalități cu titlu cominatoriu pentru a obliga furnizorii terți esențiali de servicii TIC să respecte obligațiile în materie de transparență și de acces prevăzute în prezentul regulament nu ar trebui să fie pusă în pericol de dificultățile generate de executarea respectivelor penalități în legătură cu furnizorii terți esențiali de servicii TIC stabiliți într-o țară terță. Pentru a asigura caracterul executoriu al unor astfel de penalități și pentru a permite o punere în aplicare rapidă a procedurilor care susțin dreptul la apărare al furnizorilor terți esențiali de servicii TIC în contextul mecanismului de desemnare și al emiterii de recomandări, respectivii furnizorii terți esențiali de servicii TIC care furnizează entităților financiare servicii care afectează furnizarea de servicii financiare ar trebui să aibă obligația de a menține o prezență comercială adecvată în Uniune. Având în vedere natura supravegherii și absența unor mecanisme comparabile în alte jurisdicții, nu există mecanisme alternative adecvate care să asigure acest obiectiv prin intermediul unei cooperări eficace cu autoritățile de supraveghere financiară din țările terțe în ceea ce privește monitorizarea impactului riscurilor operaționale digitale prezentate de furnizorii terți de servicii TIC cu impact sistemic, care pot fi calificați drept furnizori terți esențiali de servicii TIC stabiliți într-o țară terță. Prin urmare, pentru a continua furnizarea de servicii TIC către entități financiare din Uniune, un furnizor terț de servicii TIC stabilit într-o țară terță care a fost desemnat ca fiind esențial în conformitate cu prezentul regulament ar trebui să întreprindă, în termen de 12 luni de la desemnarea sa, toate măsurile necesare pentru a asigura stabilirea sa în Uniune, prin înființarea unei filiale, astfel cum este definită în întregul acquis al Uniunii, și anume în Directiva 2013/34/UE a Parlamentului European și a Consiliului ([21]).

(82) Cerința de a înființa o filială în Uniune nu ar trebui să împiedice furnizorul terț esențial de servicii TIC să furnizeze servicii TIC și asistența tehnică aferentă de la instalații și infrastructuri situate în afara Uniunii. Prezentul regulament nu impune o obligație de localizare a datelor, deoarece nu impune stocarea sau prelucrarea datelor în Uniune.

(83) Furnizorii terți esențiali de servicii TIC ar trebui să fie în măsură să furnizeze servicii TIC oriunde în lume, nu neapărat sau nu numai de la sedii situate în Uniune. Activitățile de supraveghere ar trebui să se desfășoare mai întâi la sediile situate în Uniune și prin interacțiunea cu entități situate în Uniune, inclusiv cu filialele înființate de furnizori terți esențiali de servicii TIC în temeiul prezentului regulament. Cu toate acestea, astfel de acțiuni în cadrul Uniunii ar putea fi insuficiente pentru a permite supraveghetorului principal să își îndeplinească pe deplin și în mod eficace sarcinile care îi revin în temeiul prezentului regulament. Prin urmare, supraveghetorul principal ar trebui să fie, de asemenea, în măsură să își exercite competențele de supraveghere relevante în țări terțe. Exercitarea acestor competențe în țări terțe ar trebui să permită supraveghetorului principal să examineze instalațiile de la care serviciile TIC sau de asistență tehnică sunt efectiv furnizate sau gestionate de furnizorul terț esențial de servicii TIC și ar trebui să ofere supraveghetorului principal o înțelegere cuprinzătoare și operațională a gestionării riscurilor TIC de către furnizorul terț esențial de servicii TIC. Posibilitatea ca supraveghetorul principal, în calitate de agenție a Uniunii, să exercite competențe în afara teritoriului Uniunii ar trebui să fie încadrată în mod corespunzător de condițiile relevante, în special de consimțământul furnizorului terț esențial de servicii TIC în cauză. În mod similar, autoritățile relevante din țara terță ar trebui să fie informate cu privire la exercitarea, pe teritoriul lor, a activităților supraveghetorului principal și nu ar trebui să aibă obiecții la aceasta. Cu toate acestea, pentru a asigura punerea în aplicare eficace și fără a aduce atingere competențelor respective ale instituțiilor Uniunii și ale statelor membre,

([21]) Directiva 2013/34/UE a Parlamentului European și a Consiliului din 26 iunie 2013 privind situațiile financiare anuale, situațiile financiare consolidate și rapoartele conexe ale anumitor tipuri de întreprinderi, de modificare a Directivei 2006/43/CE a Parlamentului European și a Consiliului și de abrogare a Directivelor 78/660/CEE și 83/349/CEE ale Consiliului (JO L 182, 29.6.2013, p. 19).

aceste competențe trebuie, de asemenea, să fie pe deplin ancorate în încheierea acordurilor de cooperare administrativă cu autoritățile relevante din țara terță în cauză. Prin urmare, prezentul regulament ar trebui să permită AES să încheie acorduri de cooperare administrativă cu autoritățile relevante din țări terțe, care nu ar trebui să creeze obligații juridice în ceea ce privește Uniunea și statele sale membre.

(84) Pentru a facilita comunicarea cu supraveghetorul principal și pentru a asigura o reprezentare adecvată, furnizorii terți esențiali de servicii TIC care fac parte dintr-un grup ar trebui să desemneze o persoană juridică drept punct de coordonare.

(85) Cadrul de supraveghere nu ar trebui să aducă atingere competenței statelor membre de a derula propriile misiuni de supraveghere sau monitorizare cu privire la furnizorii terți de servicii TIC care nu sunt desemnați ca fiind esențiali în temeiul prezentului regulament, dar care sunt considerați importanți la nivel național.

(86) Pentru a valorifica arhitectura instituțională multistratificată 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. Acesta ar trebui să fie 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 emiterea de recomandări colective, în special cu privire la analiza comparativă a programelor de supraveghere pentru furnizorii terți esențiali de servicii TIC, precum și pentru identificarea celor mai bune practici pentru abordarea aspectelor legate de riscul de concentrare a TIC.

(87) Pentru a se asigura că furnizorii terți esențiali de servicii TIC sunt supravegheați în mod adecvat și eficace la nivelul Uniunii, prezentul regulament prevede că oricare dintre cele trei AES ar putea fi desemnată drept supraveghetor principal. Atribuirea individuală a unui furnizor terț esențial de servicii TIC uneia dintre cele trei AES ar trebui să rezulte dintr-o evaluare a preponderenței entităților financiare care își desfășoară activitatea în sectoarele financiare pentru care AES respectivă are atribuții. Această abordare ar trebui să conducă la o repartizare echilibrată a sarcinilor și atribuțiilor între cele trei AES, în contextul exercitării funcțiilor de supraveghere, și ar trebui să utilizeze în mod optim resursele umane și expertiza tehnică disponibile în fiecare dintre cele trei AES.

(88) Supraveghetorilor principali ar trebui să li se acorde competențele necesare pentru a efectua investigații, pentru a desfășura inspecții la fața locului și în afara sediului la sediile și locațiile furnizorilor terți esențiali de servicii TIC și pentru a obține informații complete și actualizate. Aceste competențe ar trebui să îi permită supraveghetorului principal să obțină informații concrete cu privire la tipul, dimensiunea și impactul riscurilor TIC generate de părți terțe pentru entitățile financiare și, în cele din urmă, pentru sistemul financiar al Uniunii. Încredințarea rolului principal de supraveghere AES este o condiție prealabilă pentru înțelegerea și abordarea dimensiunii sistemice a riscurilor TIC în domeniul financiar. Impactul furnizorilor terți esențiali de servicii TIC asupra sectorului serviciilor financiare din Uniune și potențialele probleme cauzate de riscul asociat de concentrare a TIC impun adoptarea unei abordări colective la nivelul Uniunii. Efectuarea simultană a mai multor misiuni de audit și exercitarea simultană a mai multor drepturi de acces, efectuate separat de numeroase autorități competente, cu o coordonare redusă sau inexistentă între acestea, ar împiedica supraveghetorii financiari să obțină o imagine de ansamblu completă și cuprinzătoare a riscurilor TIC generate de părți terțe în Uniune, creând în același timp redundanță, sarcini și complexitate pentru furnizorii terți esențiali de servicii TIC în cazul în care aceștia ar face obiectul a numeroase cereri de monitorizare și inspecție.

(89) Având în vedere impactul semnificativ al desemnării lor ca fiind esențiali, prezentul regulament ar trebui să asigure respectarea drepturilor furnizorilor terți esențiali de servicii TIC pe tot parcursul punerii în aplicare a cadrului de supraveghere. Înainte de a fi desemnați drept esențiali, furnizorii respectivi ar trebui, de exemplu, să aibă dreptul să prezinte supraveghetorului principal o declarație motivată care să conțină orice informații relevante în scopul evaluării legate de desemnarea lor. Întrucât supraveghetorul principal ar trebui să fie împuternicit să prezinte recomandări cu privire la aspecte legate de riscurile TIC și la măsurile reparatorii adecvate, care includ competența de a se opune anumitor acorduri contractuale care afectează în ultimă instanță stabilitatea entității financiare sau a sistemului financiar; furnizorilor terți esențiali de servicii TIC ar trebui, de asemenea, să li se ofere posibilitatea de a furniza, înainte de finalizarea recomandărilor respective, explicații cu privire la impactul preconizat al soluțiilor avute în vedere în recomandări asupra clienților care sunt entități care nu intră în domeniul de aplicare al

prezentului regulament și să formuleze soluții pentru atenuarea riscurilor. Furnizorii terți esențiali de servicii TIC care nu sunt de acord cu recomandările ar trebui să prezinte o explicație motivată a intenției lor de a nu aproba recomandarea. În cazul în care nu se prezintă o astfel de explicație motivată sau explicația motivată este considerată insuficientă, supraveghetorul principal ar trebui să emită un anunț public care să descrie succint problema neconformității.

(90) Autoritățile competente ar trebui să includă în mod corespunzător sarcina de a verifica respectarea pe fond a recomandărilor emise de supraveghetorul principal în funcțiile lor cu privire la supravegherea prudențială a entităților financiare. Autoritățile competente ar trebui să poată solicita entităților financiare să ia măsuri suplimentare pentru a aborda riscurile identificate în recomandările supraveghetorului principal și ar trebui să emită, în timp util, notificări în acest sens. În cazul în care supraveghetorul principal adresează recomandări furnizorilor terți esențiali de servicii TIC care sunt supravegheați în temeiul Directivei (UE) 2022/2555, autoritățile competente ar trebui să poată consulta, în mod voluntar și înainte de a adopta măsuri suplimentare, autoritățile competente în temeiul directivei respective pentru a promova o abordare coordonată în ceea ce privește furnizorii terți esențiali de servicii TIC în cauză.

(91) Exercitarea supravegherii ar trebui să fie ghidată de trei principii operaționale menite să asigure: (a) o coordonare strânsă între AES în rolurile lor de supraveghetori principali, prin intermediul unei rețele de supraveghere comună (RSC), (b) coerența cu cadrul instituit prin Directiva (UE) 2022/2555 (printr-o consultare voluntară a organismelor în temeiul directivei respective pentru a evita duplicarea măsurilor care vizează furnizorii terți esențiali de servicii TIC) și (c) aplicarea diligenței pentru a reduce la minimum riscul potențial de perturbare a serviciilor furnizate de furnizorii terți esențiali de servicii TIC clienților care sunt entități exceptate din domeniul de aplicare al prezentului regulament.

(92) Cadrul de supraveghere nu ar trebui să înlocuiască sau să substituie în niciun fel sau parțial cerința ca entitățile financiare să gestioneze ele însele riscurile generate de utilizarea furnizorilor terți de servicii TIC, inclusiv obligația acestora de a menține o monitorizare continuă a acordurilor contractuale încheiate cu furnizorii terți esențiali de servicii TIC. În mod similar, cadrul de supraveghere nu ar trebui să afecteze responsabilitatea deplină a entităților financiare de respectare și îndeplinire a tuturor obligațiilor legale prevăzute în prezentul regulament și în dreptul relevant privind serviciile financiare.

(93) 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 și ar trebui, în acest sens, să se bazeze pe evaluarea relevantă a supraveghetorului principal. Orice măsuri ar trebui, în orice caz, să fie coordonate și convenite în prealabil cu supraveghetorul principal în contextul exercitării sarcinilor din cadrul de supraveghere.

(94) Pentru a promova convergența la nivel internațional în ceea ce privește utilizarea celor mai bune practici în revizuirea și monitorizarea gestionării riscurilor digitale de către furnizorii terți de servicii TIC, AES ar trebui încurajate să încheie acorduri de cooperare cu autoritățile relevante de supraveghere și de reglementare din țări terțe.

(95) Pentru a valorifica competențele, aptitudinile tehnice și expertiza specifice ale personalului specializat în riscurile operaționale și cele legate de TIC din cadrul autorităților competente, din cadrul celor trei AES și, în mod voluntar, din cadrul autorităților competente în temeiul Directivei (UE) 2022/2555, supraveghetorul principal ar trebui să se bazeze pe capacitățile și cunoștințele naționale de supraveghere și să înființeze echipe specializate de examinare pentru fiecare furnizor terț esențial de servicii TIC, reunind echipe multidisciplinare în sprijinul pregătirii și executării activităților de supraveghere, inclusiv al investigațiilor și inspecțiilor generale ale furnizorilor terți esențiali de servicii TIC, precum și pentru orice acțiuni ulterioare necesare în acest sens.

(96) Deși costurile care rezultă din sarcinile de supraveghere ar urma să fie finanțate integral din taxele percepute furnizorilor terți esențiali de servicii TIC, este totuși probabil ca AES să suporte, înainte de începerea cadrului de supraveghere, costuri pentru punerea în aplicare a unor sisteme TIC specifice care să sprijine supravegherea viitoare, deoarece sistemele TIC specifice ar trebui să fie dezvoltate și implementate în prealabil. Prin urmare, prezentul regulament prevede un model de finanțare hibrid, prin care cadrul de supraveghere ar fi, ca atare, finanțat integral din taxe, în timp ce dezvoltarea sistemelor TIC ale AES ar fi finanțată din contribuțiile Uniunii și ale autorităților naționale competente.

(97) Autoritățile competente ar trebui să dispună de toate competențele de supraveghere, de investigare și de sancționare necesare pentru a asigura exercitarea corespunzătoare a atribuțiilor care le revin în temeiul prezentului regulament. Acestea ar trebui, în principiu, să publice anunțuri privind sancțiunile administrative pe care le impun. Întrucât entitățile financiare și furnizorii terți de servicii TIC pot fi stabiliți în state membre diferite și pot fi supravegheați de autorități competente diferite, aplicarea prezentului regulament ar trebui să fie facilitată, pe de o parte, printr-o cooperare strânsă între autoritățile competente relevante, inclusiv BCE în ceea ce privește atribuțiile specifice care îi sunt conferite prin Regulamentul (UE) nr. 1024/2013 al Consiliului și, pe de altă parte, prin consultarea cu AES prin intermediul schimbului reciproc de informații și prin furnizarea de asistență în contextul activităților de supraveghere relevante.

(98) Pentru a cuantifica și a califica suplimentar criteriile pentru desemnarea furnizorilor terți de servicii TIC ca fiind esențiali și pentru a armoniza taxele de supraveghere, competența de a adopta acte în conformitate cu articolul 290 din TFUE ar trebui delegată Comisiei pentru a completa prezentul regulament, pentru a preciza mai în detaliu impactul sistemic pe care l-ar putea avea o defecțiune sau o întrerupere operațională a unui furnizor terț de servicii TIC asupra entităților financiare cărora le furnizează servicii TIC, numărul de instituții globale de importanță sistemică (G-SII) sau de alte instituții de importanță sistemică (O-SII), care se bazează pe furnizorul terț de servicii TIC în cauză, numărul furnizorilor terți de servicii TIC activi pe o anumită piață, costurile aferente migrării datelor și sarcinilor TIC către alți furnizori terți de servicii TIC, precum și cuantumul taxelor de supraveghere și modul în care acestea trebuie plătite. 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 interinstituțional din 13 aprilie 2016 privind o mai bună legiferare ([22]). În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul ar trebui să primească toate documentele în același timp cu experții din statele membre, iar experții acestor instituții ar trebui să aibă acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

(99) Standardele tehnice de reglementare ar trebui să asigure armonizarea consecventă a cerințelor prevăzute în prezentul regulament. În rolurile lor de organisme care dispun de o expertiză foarte specializată, AES ar trebui să elaboreze proiecte de standarde tehnice de reglementare care nu implică opțiuni de politică, pe care să le prezinte Comisiei. Ar trebui elaborate standarde tehnice de reglementare în domeniul gestionării riscurilor TIC, al raportării incidentelor majore legate de TIC, al testării, precum și în ceea ce privește cerințele-cheie pentru o monitorizare riguroasă a riscurilor TIC generate de părți terțe. Comisia și AES ar trebui să se asigure că standardele și cerințele respective pot fi aplicate de toate entitățile financiare într-un mod proporțional cu dimensiunea și profilul lor general de risc, precum și cu natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor. Comisia ar trebui să fie împuternicită să adopte aceste standarde tehnice de reglementare prin intermediul unor acte delegate în temeiul articolului 290 din TFUE și al articolelor 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

(100) Pentru a facilita comparabilitatea rapoartelor privind incidentele majore legate de TIC și incidentele operaționale sau de securitate majore legate de plăți, precum și pentru a asigura transparența cu privire la acordurile contractuale pentru utilizarea serviciilor TIC furnizate de furnizorii terți de servicii TIC, AES ar trebui să elaboreze proiecte de standarde tehnice de punere în aplicare care să stabilească modele, formulare și proceduri standardizate prin care entitățile financiare să raporteze un incident major legat de TIC și un incident operațional sau de securitate major legat de plăți, precum și modele standardizate pentru înregistrarea informațiilor. Atunci când elaborează standardele respective, AES ar trebui să ia în considerare dimensiunea și profilul general de risc al entității financiare, precum și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor sale. 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 în conformitate cu articolul 15 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

([22]) JO L 123, 12.5.2016, p. 1.

(101) 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 ([23]), (UE) nr. 648/2012 ([24]), (UE) nr. 600/2014 ([25]) și (UE) nr. 909/2014 ([26]) ale Parlamentului European și ale Consiliului, 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.

(102) Întrucât prezentul regulament, împreună cu Directiva (UE) 2022/2556 a Parlamentului European și a Consiliului ([27]), 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 și Regulamentul (UE) 2016/1011 al Parlamentului European și al Consiliului ([28]), pentru a se asigura coerența deplină, regulamentele respective ar trebui să fie modificate pentru a clarifica faptul că dispozițiile aplicabile legate de riscurile TIC sunt prevăzute în prezentul regulament.

(103) În consecință, domeniul de aplicare al articolelor relevante referitoare la riscul operațional, pe baza cărora delegările de competențe prevăzute în Regulamentele (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 au prevăzut adoptarea de acte delegate și de punere în aplicare, ar trebui să fie restrâns în vederea transferării în prezentul regulament a tuturor dispozițiilor care acoperă aspectele legate de reziliența operațională digitală care fac parte în prezent din regulamentele respective.

(104) Riscul cibernetic sistemic potențial asociat cu utilizarea infrastructurilor TIC care permit operarea sistemelor de plată și furnizarea de activități de prelucrare a plăților ar trebui să fie abordat în mod corespunzător la nivelul Uniunii prin norme armonizate în materie de reziliență digitală. În acest scop, Comisia ar trebui să evalueze rapid necesitatea revizuirii domeniului de aplicare al prezentului regulament, aliniind în același timp această revizuire la rezultatul revizuirii cuprinzătoare prevăzute în Directiva (UE) 2015/2366. Numeroasele atacuri la scară largă din ultimul deceniu demonstrează măsura în care sistemele de plată au ajuns să fie expuse în fața amenințările cibernetice. Plasate în centrul lanțului de servicii de plată și prezentând interconexiuni puternice cu sistemul financiar general, sistemele de plată și activitățile de procesare a plăților au dobândit o importanță critică pentru funcționarea piețelor financiare ale Uniunii. Atacurile cibernetice asupra unor astfel de sisteme pot provoca perturbări operaționale grave ale activității, cu repercusiuni directe asupra funcțiilor economice esențiale, cum ar fi facilitarea plăților, și efecte indirecte asupra proceselor economice conexe. Până la instituirea la nivelul Uniunii a unui regim armonizat și a supravegherii operatorilor de sisteme de plată și a entităților de prelucrare, statele membre pot, în vederea aplicării unor practici de piață similare, să se inspire din cerințele privind reziliența operațională digitală prevăzute în prezentul regulament, atunci când aplică norme operatorilor de sisteme de plată și entităților de prelucrare supravegheate în jurisdicțiile lor.

([23]) Regulamentul (CE) nr. 1060/2009 al Parlamentului European și al Consiliului din 16 septembrie 2009 privind agențiile de rating de credit (JO L 302, 17.11.2009, p. 1).

([24]) Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului din 4 iulie 2012 privind instrumentele financiare derivate extrabursiere, contrapărțile centrale și registrele centrale de tranzacții (JO L 201, 27.7.2012, p. 1).

([25]) Regulamentul (UE) nr. 600/2014 al Parlamentului European și al Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Regulamentului (UE) nr. 648/2012 (JO L 173, 12.6.2014, p. 84).

([26]) Regulamentul (UE) nr. 909/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind îmbunătățirea decontării titlurilor de valoare în Uniunea Europeană și privind depozitarii centrali de titluri de valoare și de modificare a Directivelor 98/26/CE și 2014/65/UE și a Regulamentului (UE) nr. 236/2012 (JO L 257, 28.8.2014, p. 1).

([27]) Directiva (UE) 2022/2556 a Parlamentului European și a Consiliului din 14 decembrie 2022 de modificare a Directivelor 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 și (UE) 2016/2341 în ceea ce privește reziliența operațională digitală pentru sectorul financiar (a se vedea pagina 153 din prezentul Jurnal Oficial).

([28]) 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).

(105) Întrucât obiectivul prezentului regulament, și anume atingerea unui nivel ridicat de reziliență operațională digitală pentru entitățile financiare reglementate, nu poate fi realizat în mod satisfăcător de către statele membre deoarece necesită armonizarea diferitelor norme din dreptul Uniunii și din dreptul intern, dar, având în vedere amploarea și efectele sale, poate fi realizat mai bine la nivelul Uniunii, aceasta poate adopta măsuri în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru atingerea obiectivului respectiv.

(106) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([29]) și a emis un aviz la 10 mai 2021 ([30]),

ADOPTĂ PREZENTUL REGULAMENT:

*CAPITOLUL I*

***Dispoziții generale***

*Articolul 1*

**Obiectul**

(1) Pentru a atinge un nivel comun ridicat de reziliență operațională digitală, prezentul regulament stabilește cerințe uniforme privind securitatea rețelelor și a sistemelor informatice care sprijină procesele operaționale ale entităților financiare, după cum urmează:

(a) cerințe aplicabile entităților financiare în legătură cu:

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

(ii) raportarea incidentelor majore legate de TIC și notificarea, în mod voluntar, a amenințărilor cibernetice semnificative către autoritățile competente;

(iii) raportarea de către entitățile financiare menționate la articolul 2 alineatul (1) literele (a)-(d) către autoritățile competente a incidentelor operaționale sau de securitate majore legate de plăți;

(iv) testarea rezilienței operaționale digitale;

(v) schimbul de informații și de date operative cu privire la amenințările cibernetice și vulnerabilități;

(vi) măsuri pentru buna gestionare 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) reguli privind instituirea și desfășurarea cadrului de supraveghere pentru furnizorii terți esențiali de servicii TIC, atunci când furnizează servicii entităților financiare;

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

(2) În ceea ce privește entitățile financiare identificate drept entități esențiale sau importante în temeiul normelor naționale care transpun articolul 3 din Directiva (UE) 2022/2555, prezentul regulament este considerat un act juridic sectorial al Uniunii în sensul articolului 4 din directiva respectivă.

(3) Prezentul regulament nu aduce atingere responsabilității statelor membre în ceea ce privește funcțiile esențiale ale statului cu privire la siguranța publică, apărarea și securitatea națională, în conformitate cu dreptul Uniunii.

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

([30]) JO C 229, 15.6.2021, p. 16.

*Articolul 2*

**Domeniul de aplicare**

(1) Fără a aduce atingere alineatelor (3) și (4), prezentul regulament se aplică următoarelor entități:

(a) instituțiile de credit;

(b) instituțiile de plată, inclusiv instituțiile de plată exceptate în temeiul Directivei (UE) 2015/2366;

(c) prestatorii de servicii de informare cu privire la conturi;

(d) instituțiile emitente de monedă electronică, inclusiv instituțiile emitente de monedă electronică exceptate în temeiul Directivei 2009/110/CE;

(e) firmele de investiții;

(f) prestatorii de servicii de criptoactive autorizați în temeiul unui regulament al Parlamentului European și al Consiliului privind piețele criptoactivelor și de modificare a Regulamentelor (UE) nr. 1093/2010 și (UE) nr. 1095/2010 și a Directivelor 2013/36/UE și (UE) 2019/1937 (denumit în continuare „Regulamentul privind piețele criptoactivelor") și emitenții de tokenuri raportate la active;

(g) depozitarii centrali de titluri de valoare;

(h) contrapărțile centrale;

(i) locurile de tranzacționare;

(j) registrele centrale de tranzacții;

(k) administratorii de fonduri de investiții alternative;

(l) societățile de administrare;

(m) furnizorii de servicii de raportare a datelor;

(n) întreprinderile de asigurare și de reasigurare;

(o) intermediarii de asigurări, intermediarii de reasigurări și intermediarii de asigurări auxiliare;

(p) instituțiile pentru furnizarea de pensii ocupaționale;

(q) agențiile de rating de credit;

(r) administratorii de indici de referință critici;

(s) furnizorii de servicii de finanțare participativă;

(t) registrele centrale de securitizări;

(u) furnizorii terți de servicii TIC.

(2) În sensul prezentului regulament, entitățile menționate la alineatul (1) literele (a)-(t) sunt denumite colectiv „entități financiare".

(3) Prezentul regulament nu se aplică următoarelor entități:

(a) administratorii de fonduri de investiții alternative, astfel cum sunt menționați la articolul 3 alineatul (2) din Directiva 2011/61/UE;

(b) întreprinderile de asigurare și de reasigurare, astfel cum sunt menționate la articolul 4 din Directiva 2009/138/CE;

(c) instituțiile pentru furnizarea de pensii ocupaționale care gestionează sisteme de pensii care împreună nu au mai mult de 15 membri în total;

(d) persoanele fizice sau juridice exceptate în temeiul articolelor 2 și 3 din Directiva 2014/65/UE;

(e) intermediarii de asigurări, intermediarii de reasigurări și intermediarii de asigurări auxiliare care sunt microîntreprinderi sau întreprinderi mici sau mijlocii;

(f) oficiile poștale care efectuează operațiuni de virament, astfel cum sunt menționate la articolul 2 alineatul (5) punctul 3 din Directiva 2013/36/UE.

(4) Statele membre pot exclude din domeniul de aplicare al prezentului regulament entitățile menționate la articolul 2 alineatul (5) punctele 4-23 din Directiva 2013/36/UE care sunt situate pe teritoriile lor. În cazul în care un stat membru face uz de această opțiune, acesta informează Comisia cu privire la aceasta, precum și cu privire la orice modificare ulterioară. Comisia pune aceste informații la dispoziția publicului pe site-ul său sau prin alte mijloace ușor accesibile.

*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 reevalua integritatea și fiabilitatea sa operațională, prin asigurarea, în mod direct sau indirect, utilizând servicii oferite de furnizori terți de servicii TIC, a întregii game de capacități legate de TIC care sunt necesare pentru a aborda securitatea rețelelor și a sistemelor informatice utilizate de o entitate financiară și care sprijină furnizarea continuă de servicii financiare și calitatea acestora, inclusiv pe întreaga durată a perturbărilor;

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

3. „sistem TIC moștenit” înseamnă un sistem TIC ajuns la sfârșitul ciclului său de viață care nu este adecvat pentru a fi modernizat sau reparat, din motive tehnologice sau comerciale, sau pentru care furnizorul său ori un furnizor terț de servicii TIC nu mai oferă asistență, dar care încă este în uz și sprijină funcțiile entității financiare;

4. „securitatea rețelelor și a sistemelor informatice” înseamnă securitatea rețelelor și a sistemelor informatice astfel cum sunt definite la articolul 6 punctul 2 din Directiva (UE) 2022/2555;

5. „risc TIC” înseamnă orice circumstanță care poate fi identificată în mod rezonabil în legătură cu utilizarea rețelelor și a sistemelor informatice care, dacă se materializează, poate compromite securitatea rețelelor și a sistemelor informatice, a oricărui instrument sau proces dependent de tehnologie, a operațiilor și a proceselor sau a furnizării serviciilor prin crearea de efecte negative în mediul digital sau fizic;

6. „activ informațional” înseamnă o colecție de informații, materială sau imaterială, care merită protejată;

7. „activ TIC” înseamnă un activ software sau hardware din rețelele și sistemele informatice utilizate de entitatea financiară;

8. „incident legat de TIC” înseamnă un eveniment unic sau o serie de evenimente conexe neplanificate de entitatea financiară care compromit securitatea rețelelor și a sistemelor informatice și care au un impact negativ asupra disponibilității, autenticității, integrității sau confidențialității datelor sau asupra serviciilor furnizate de entitatea financiară;

9. „incident operațional sau de securitate legat de plăți” înseamnă un eveniment unic sau o serie de evenimente conexe neplanificate de entitățile financiare menționate la articolul 2 alineatul (1) literele (a)-(d), legate sau nu de TIC, care au un impact negativ asupra disponibilității, autenticității, integrității sau confidențialității datelor legate de plăți sau asupra serviciilor legate de plăți furnizate de entitatea financiară;

10. „incident major legat de TIC” înseamnă un incident legat de TIC care are un impact negativ puternic asupra rețelelor și sistemelor informatice care sprijină funcțiile critice sau importante ale entității financiare;

11. „incident major operațional sau de securitate legat de plăți” înseamnă un incident operațional sau de securitate legat de plăți care are un efect negativ puternic asupra serviciilor legate de plăți furnizate;

12. „amenințare cibernetică” înseamnă amenințare cibernetică astfel cum este definită la articolul 2 punctul 8 din Regulamentul (UE) 2019/881;

13. „amenințare cibernetică semnificativă” înseamnă o amenințare cibernetică ale cărei caracteristici tehnice indică faptul că ar putea avea ca rezultat un incident major legat de TIC sau un incident major operațional sau de securitate legat de plăți;

14. „atac cibernetic” înseamnă un incident rău-intenționat legat de TIC, cauzat prin intermediul unei tentative comise de un factor perturbator care generează amenințări 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;

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

16. „vulnerabilitate” înseamnă un punct slab, o sensibilitate sau un defect al unui activ, sistem, proces sau control care poate fi exploatat;

17. „teste de penetrare bazate pe amenințări (TLPT)” înseamnă un cadru care imită tacticile, tehnicile și procedurile utilizate de actorii din viața reală care generează amenințări, percepute ca reprezentând o amenințare cibernetică autentică, și care asigură o testare controlată, personalizată, bazată pe date operative (de tipul „echipa roșie”) a sistemelor critice de producție în timp real ale entității financiare;

18. „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, inclusiv prin acorduri de externalizare;

19. „furnizor terț de servicii TIC” înseamnă o întreprindere care furnizează servicii TIC;

20. „furnizor de servicii TIC intragrup” înseamnă o întreprindere care face parte dintr-un grup financiar și care oferă servicii predominant TIC exclusiv entităților financiare din același grup ori entităților financiare care țin de același sistem instituțional de protecție, inclusiv societăților-mamă ale acestora, filialelor și sucursalelor sau altor entități care sunt în proprietate comună ori sub control comun;

21. „servicii TIC” înseamnă servicii digitale și de date furnizate prin intermediul sistemelor TIC către unul sau mai mulți utilizatori interni sau externi în mod continuu, inclusiv hardware ca serviciu și servicii hardware, care includ furnizarea de asistență tehnică prin actualizări de software sau firmware din partea furnizorului de hardware, cu excepția serviciilor de telefonie analogică tradiționale;

22. „funcție critică sau importantă” înseamnă o funcție a cărei întrerupere ar afecta în mod semnificativ performanța financiară a unei entități financiare sau soliditatea ori continuitatea serviciilor și activităților sale sau a cărei întrerupere, deficiență sau eșuare în executare 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 dreptului aplicabil în domeniul serviciilor financiare;

23. „furnizor terț esențial de servicii TIC” înseamnă un furnizor terț de servicii TIC desemnat drept esențial în conformitate cu articolul 31;

24. „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 și care a încheiat un acord contractual cu o entitate financiară pentru furnizarea de servicii TIC;

25. „filială” înseamnă o filială în sensul articolului 2 punctul 10 și al articolului 22 din Directiva 2013/34/UE;

26. „grup” înseamnă un grup în sensul articolului 2 punctul 11 din Directiva 2013/34/UE;

27. „societate-mamă” înseamnă o societate-mamă în sensul articolului 2 punctul 9 și al articolului 22 din Directiva 2013/34/UE;

28. „subcontractant TIC stabilit într-o țară terță” înseamnă un subcontractant TIC care este o persoană juridică stabilită într-o țară terță 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;

29. „risc de concentrare a serviciilor TIC” înseamnă o expunere la furnizori terți esențiali de servicii TIC individuali sau multipli relaționați, care creează un grad de dependență față de astfel de furnizori, astfel încât indisponibilitatea, intrarea în dificultate sau alt tip de deficiență a acestor furnizori poate pune în pericol capacitatea unei entități financiare de a oferi funcții critice sau importante ori ar putea genera alte tipuri de efecte negative pentru aceasta, inclusiv pierderi mari sau poate pune în pericol stabilitatea financiară a Uniunii în ansamblu;

30. „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 a Parlamentului European și al Consiliului ([31]), 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 și în dispozițiile relevante din Regulamentul privind piețele criptoactivelor, sau persoanele echivalente care conduc efectiv entitatea sau dețin funcții-cheie în conformitate cu dreptul Uniunii sau cu dreptul intern relevant;

31. „instituție de credit” înseamnă 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 ([32]);

32. „instituție de credit exceptată în temeiul Directivei 2013/36/UE” înseamnă o entitate astfel cum este menționată la articolul 2 alineatul (5) punctele 4-23 din Directiva 2013/36/UE;

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

34. „firmă de investiții mică și neinterconectată” înseamnă o firmă de investiții care îndeplinește condițiile prevăzute la articolul 12 alineatul (1) din Regulamentul (UE) 2019/2033 al Parlamentului European și al Consiliului ([33]);

35. „instituție de plată” înseamnă o instituție de plată astfel cum este definită la articolul 4 punctul 4 din Directiva (UE) 2015/2366;

36. „instituție de plată exceptată în temeiul Directivei (UE) 2015/2366” înseamnă o instituție de plată exceptată în temeiul articolului 32 alineatul (1) din Directiva (UE) 2015/2366;

37. „prestator de servicii de informare cu privire la conturi” înseamnă un prestator de servicii de informare cu privire la conturi astfel cum este menționat la articolul 33 alineatul (1) din Directiva (UE) 2015/2366;

38. „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;

39. „instituție emitentă de monedă electronică exceptată în temeiul Directivei 2009/110/CE” înseamnă o instituție emitentă de monedă electronică care beneficiază de o exceptare astfel cum se menționează la articolul 9 alineatul (1) din Directiva 2009/110/CE;

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

41. „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;

42. „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;

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

44. „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;

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

46. „furnizor de servicii de raportare a datelor” înseamnă un furnizor de servicii de raportare a datelor în sensul Regulamentului (UE) nr. 600/2014, astfel cum se menționează la articolul 2 alineatul (1) punctele 34-36;

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

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

---

([31]) Directiva 2009/65/CE a Parlamentului European și a Consiliului din 13 iulie 2009 de coordonare a actelor cu putere de lege și a actelor administrative privind organismele de plasament colectiv în valori mobiliare (OPCVM) (JO L 302, 17.11.2009, p. 32).

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

([33]) Regulamentul (UE) 2019/2033 al Parlamentului European și al Consiliului din 27 noiembrie 2019 privind cerințele prudențiale ale firmelor de investiții și de modificare a Regulamentelor (UE) nr. 1093/2010, (UE) nr. 575/2013, (UE) nr. 600/2014 și (UE) nr. 806/2014 (JO L 314, 5.12.2019, p. 1).

49. „intermediar de asigurări” înseamnă un intermediar de asigurări astfel cum este definit la articolul 2 alineatul (1) punctul 3 din Directiva (UE) 2016/97 a Parlamentului European și a Consiliului ([34]);

50. „intermediar de asigurări auxiliare” înseamnă un intermediar de asigurări auxiliare astfel cum este definit la articolul 2 alineatul (1) punctul 4 din Directiva (UE) 2016/97;

51. „intermediar de reasigurări” înseamnă un intermediar de reasigurări astfel cum este definit la articolul 2 alineatul (1) punctul 5 din Directiva (UE) 2016/97;

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

53. „instituție mică pentru furnizarea de pensii ocupaționale” înseamnă o instituție pentru furnizarea de pensii ocupaționale care gestionează scheme de pensii care împreună au mai puțin de 100 de membri în total;

54. „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;

55. „furnizor de servicii de criptoactive” înseamnă un furnizor de servicii de criptoactive astfel cum este definit în dispozițiile relevante din Regulamentul privind piețele criptoactivelor;

56. „emitent de tokenuri raportate la active” înseamnă un emitent de tokenuri raportate la active astfel cum sunt definite în dispozițiile relevante din Regulamentul privind piețele criptoactivelor;

57. „administrator de indici de referință critici” înseamnă un administrator de indici de referință critici astfel cum sunt definiți la articolul 3 alineatul (1) punctul 25 din Regulamentul (UE) 2016/1011;

58. „furnizor de servicii de finanțare participativă” înseamnă un furnizor de servicii de finanțare participativă astfel cum este definit la articolul 2 alineatul (1) litera (e) din Regulamentul (UE) 2020/1503 al Parlamentului European și al Consiliului ([35]);

59. „registru central de securitizări” înseamnă un registru central de securitizări astfel cum este definit la articolul 2 punctul 23 din Regulamentul (UE) 2017/2402 al Parlamentului European și al Consiliului ([36]);

60. „microîntreprindere” înseamnă o entitate financiară, alta decât un loc de tranzacționare, o contraparte centrală, un registru central de tranzacții sau un depozitar central de titluri de valoare, care are mai puțin de 10 angajați și o cifră de afaceri anuală și/sau un bilanț anual total care nu depășește 2 milioane EUR;

61. „supraveghetor principal” înseamnă autoritatea europeană de supraveghere desemnată în conformitate cu articolul 31 alineatul (1) litera (b) din prezentul regulament;

62. „Comitetul comun” înseamnă comitetul menționat la articolul 54 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010;

63. „întreprindere mică” înseamnă o entitate financiară care are cel puțin 10 angajați, dar mai puțin de 50 de angajați, și o cifră de afaceri anuală și/sau un bilanț anual total care depășește 2 milioane EUR, dar nu depășește 10 milioane EUR;

64. „întreprindere mijlocie” înseamnă o entitate financiară care nu este o întreprindere mică și care are mai puțin de 250 de angajați și o cifră de afaceri anuală care nu depășește 50 de milioane EUR și/sau un bilanț anual care nu depășește 43 de milioane EUR;

65. „autoritate publică” înseamnă orice entitate guvernamentală sau altă entitate a administrației publice, inclusiv băncile centrale naționale.

---

([34]) Directiva (UE) 2016/97 a Parlamentului European și a Consiliului din 20 ianuarie 2016 privind distribuția de asigurări (JO L 26, 2.2.2016, p. 19).

([35]) Regulamentul (UE) 2020/1503 al Parlamentului European și al Consiliului din 7 octombrie 2020 privind furnizorii europeni de servicii de finanțare participativă pentru afaceri și de modificare a Regulamentului (UE) 2017/1129 și a Directivei (UE) 2019/1937 (JO L 347, 20.10.2020, p. 1).

([36]) Regulamentul (UE) 2017/2402 al Parlamentului European și al Consiliului din 12 decembrie 2017 de stabilire a unui cadru general privind securitizarea și de creare a unui cadru specific pentru o securitizare simplă, transparentă și standardizată, și de modificare a Directivelor 2009/65/CE, 2009/138/CE și 2011/61/UE, precum și a Regulamentelor (CE) nr. 1060/2009 și (UE) nr. 648/2012 (JO L 347, 28.12.2017, p. 35).

*Articolul 4*

**Principiul proporționalității**

(1) Entitățile financiare pun în aplicare normele prevăzute la capitolul II în conformitate cu principiul proporționalității, luând în considerare dimensiunea și profilul lor general de risc și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor.

(2) În plus, entitățile financiare aplică capitolele III și IV și capitolul V secțiunea I proporțional cu dimensiunea și profilul lor general de risc și cu natura, amploarea și complexitatea serviciilor, activităților și operațiunilor lor, astfel cum se prevede în mod specific în normele relevante din capitolele respective.

(3) Autoritățile competente iau în considerare aplicarea principiului proporționalității de către entitățile financiare atunci când revizuiesc coerența cadrului de gestionare a riscurilor TIC pe baza rapoartelor prezentate la cererea autorităților competente în temeiul articolului 6 alineatul (5) și al articolului 16 alineatul (2).

*CAPITOLUL II*

***Gestionarea riscurilor TIC***

Secțiunea I

*Articolul 5*

**Guvernanță și organizare**

(1) Entitățile financiare dispun de un cadru intern de guvernanță și control care asigură o gestionare eficace și prudentă a riscurilor TIC, în conformitate cu articolul 6 alineatul (4), cu scopul de a obține un nivel ridicat de reziliență operațională digitală.

(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 6 alineatul (1).

În scopul aplicării primului paragraf, organul de conducere:

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

(b) stabilește politici menite să asigure menținerea unor standarde ridicate de disponibilitate, autenticitate, integritate și confidențialitate a datelor;

(c) stabilește roluri și responsabilități clare pentru toate funcțiile legate de TIC și instituie mecanisme de guvernanță adecvate pentru a asigura comunicarea, cooperarea și coordonarea eficace și în timp util între aceste funcții;

(d) poartă responsabilitatea generală pentru stabilirea și aprobarea strategiei privind reziliența operațională digitală, astfel cum este menționată la articolul 6 alineatul (8), inclusiv pentru determinarea nivelul adecvat de toleranță la risc pentru riscurile TIC în cazul entității financiare, astfel cum este menționată la articolul 6 alineatul (8) litera (b);

(e) aprobă, supraveghează și verifică periodic punerea în aplicare a politicii de continuitate a activității TIC și a planurilor de răspuns și de recuperare în domeniul TIC ale entității financiare, menționate la articolul 11 alineatul (1) și, respectiv, alineatul (3), care pot fi adoptate sub forma unei politici specifice dedicate care să facă parte integrantă din politica generală de continuitate a activității și planul general de răspuns și de recuperare ale entității financiare;

(f) aprobă și verifică periodic planurile de audit intern TIC și auditurile TIC ale entității financiare, precum și modificările semnificative aduse acestora;

(g) 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 programe de conștientizare cu privire la securitatea TIC și cursuri de formare în domeniul rezilienței operaționale digitale relevante menționate la articolul 13 alineatul (6), precum și competențe TIC pentru toți membrii personalului;

(h) aprobă și verifică periodic politica entității financiare cu privire la acordurile privind utilizarea serviciilor TIC furnizate de furnizori terți de servicii TIC;

(i) instituie, la nivel corporativ, canale de raportare care să îi permită să fie informat în mod corespunzător cu privire la:

(i) acordurile încheiate cu furnizorii terți de servicii TIC privind utilizarea serviciilor TIC;

(ii) orice modificări semnificative planificate relevante privind furnizorii terți de servicii TIC;

(iii) impactul potențial al unor astfel de modificări asupra funcțiilor critice sau importante care fac obiectul acordurilor respective, inclusiv un rezumat al analizei de risc pentru a evalua impactul modificărilor respective, și cel puțin incidentele majore legate de TIC și impactul acestora, precum și cu privire la măsurile de răspuns, de recuperare și corective.

(3) Entitățile financiare, altele decât microîntreprinderile, stabilesc un rol pentru a monitoriza acordurile 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 al entității financiare își actualizează în mod activ cunoștințele și competențele pentru a înțelege și a evalua riscurile TIC și impactul acestora asupra operațiunilor entității financiare, inclusiv prin frecventarea cu regularitate a unor cursuri de formare specifice, pe măsura riscurilor TIC gestionate.

Secțiunea II

*Articolul 6*

**Cadrul de gestionare a riscurilor TIC**

(1) Entitățile financiare dispun de un cadru solid, cuprinzător și bine documentat de gestionare a riscurilor TIC, ca parte a sistemului lor general de gestionare a riscurilor, care le permite să abordeze riscurile TIC în mod rapid, eficient și cuprinzător și să asigure un nivel ridicat de reziliență operațională digitală.

(2) Cadrul de gestionare a riscurilor TIC include cel puțin strategii, politici, proceduri, precum și protocoale și instrumente TIC care sunt necesare pentru a proteja în mod corespunzător și adecvat toate activele informaționale și toate activele TIC, inclusiv software pentru calculatoare, hardware și servere, precum și pentru a proteja toate componentele și infrastructurile fizice relevante, precum sediile, centrele de date și zonele desemnate sensibile, pentru a asigura că toate activele informaționale și toate activele TIC sunt protejate în mod adecvat împotriva riscurilor, inclusiv împotriva pagubelor și a accesului sau utilizării neautorizate.

(3) În conformitate cu cadrul lor de gestionare a riscurilor TIC, entitățile financiare reduc la minimum impactul riscurilor TIC prin utilizarea unor strategii, politici, proceduri, protocoale și instrumente TIC adecvate. Acestea furnizează autorităților competente, la cererea acestora, informații complete și actualizate cu privire la riscurile TIC și la cadrul lor de gestionare a riscurilor TIC.

(4) Entitățile financiare, altele decât microîntreprinderile, atribuie responsabilitatea pentru gestionarea și supravegherea riscurilor TIC unei funcții de control și asigură independența acestei funcții de control la un nivel adecvat, pentru a evita conflictele de interese. Entitățile financiare asigură în mod adecvat separarea și independența 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.

(5) Cadrul de gestionare a riscurilor TIC se documentează și se revizuiește cel puțin o dată pe an, sau periodic în cazul microîntreprinderilor, precum și în cazul unor incidente majore legate de TIC și în urma instrucțiunilor sau concluziilor în materie de supraveghere care decurg din testarea relevantă a rezilienței operaționale digitale sau din procesele de audit relevante. Acesta este îmbunătățit în permanență, pe baza învățămintelor desprinse în urma punerii în aplicare și a monitorizării. Autorității competente i se prezintă, la cererea sa, un raport privind revizuirea cadrului de gestionare a riscurilor TIC.

(6) Cadrul de gestionare a riscurilor TIC al entităților financiare, altele decât microîntreprinderile, este supus auditului intern de către auditori în mod regulat, în conformitate cu planul de audit al entităților financiare. Auditorii respectivi dețin suficiente cunoștințe, competențe și expertiză în ceea ce privește riscurile TIC, precum și o independență adecvată. Frecvența și obiectivul auditurilor TIC sunt proporționale cu riscurile TIC ale entităților financiare.

(7) Pe baza concluziilor evaluării de audit intern, entitățile financiare stabilesc un proces formal de urmărire, care include reguli pentru verificarea și remedierea în timp util a elementelor critice constatate în cadrul auditurilor TIC.

(8) Cadrul de gestionare a riscurilor TIC include o strategie privind reziliența operațională digitală, care stabilește modul de punere în aplicare a cadrului. În acest scop, strategia privind reziliența operațională digitală include metode 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 impact pentru perturbările TIC;

(c) stabilirea unor obiective clare privind securitatea informațiilor, inclusiv indicatori-cheie de performanță și indicatori-cheie de risc;

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

(e) prezentarea diferitelor mecanisme instituite pentru a detecta incidentele legate de TIC, a preveni impactul acestora și a asigura protecție împotriva acestora;

(f) evidențierea situației actuale a rezilienței operaționale digitale pe baza numărului de incidente majore legate de TIC raportate și a eficacității măsurilor preventive;

(g) implementarea testării rezilienței operaționale digitale, în conformitate cu capitolul IV din prezentul regulament;

(h) conturarea unei strategii de comunicare în cazul producerii unor incidente legate de TIC cu privire la care este necesară informarea în conformitate cu articolul 14.

(9) Entitățile financiare pot defini, în contextul strategiei privind reziliența operațională digitală menționate la alineatul (8), o strategie TIC cuprinzătoare privind existența mai multor furnizori, la nivel de grup sau de entitate, care să prezinte 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 TIC.

(10) Entitățile financiare pot externaliza, în conformitate cu legislația sectorială a Uniunii și cea națională, sarcinile de verificare a conformității cu cerințele de gestionare a riscurilor TIC către entități intragrup sau externe. În cazul unei astfel de externalizări, entitatea financiară rămâne pe deplin responsabilă de verificarea conformității cu cerințele de gestionare a riscurilor TIC.

*Articolul 7*

**Sisteme, protocoale și instrumente TIC**

Pentru a aborda și a gestiona riscurile TIC, entitățile financiare utilizează și mențin sisteme, protocoale și instrumente TIC actualizate care sunt:

(a) adecvate magnitudinii operațiunilor care sprijină desfășurarea activităților lor, în conformitate cu principiul proporționalității astfel cum este menționat la articolul 4;

(b) fiabile;

(c) dotate cu suficientă capacitate de 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) reziliente din punct de vedere tehnologic pentru a face față în mod adecvat nevoilor suplimentare de prelucrare a informațiilor, calitate necesară în condiții de criză a pieței sau în alte situații adverse.

*Articolul 8*

**Identificare**

(1) Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1), entitățile financiare identifică, clasifică și documentează în mod corespunzător toate funcțiile operaționale și toate rolurile și responsabilitățile sprijinite de TIC, activele informaționale și activele TIC care sprijină funcțiile respective, precum și rolurile și dependențele lor în legătură cu riscurile TIC. Entitățile financiare revizuiesc după caz, dar cel puțin anual, caracterul adecvat al acestei clasificări și al oricărei documentări 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 lor operaționale sprijinite de TIC, activele lor informaționale și activele lor TIC. 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 și proceselor sau procedurilor care le afectează funcțiile operaționale sprijinite de TIC, activele informaționale sau activele TIC.

(4) Entitățile financiare identifică toate activele informaționale și activele TIC, inclusiv cele din locații aflate la distanță, resursele de rețea și echipamentele hardware și le inventariază pe cele considerate esențiale. Acestea cartografiază configurația activelor informaționale și a activelor TIC și legăturile și interdependențele dintre diferitele active informaționale și active TIC.

(5) Entitățile financiare identifică și documentează toate procesele care depind de furnizori terți de servicii TIC și identifică interconexiunile cu furnizori terți de servicii TIC care oferă servicii care sprijină funcții critice sau importante.

(6) În scopul aplicării alineatelor (1), (4) și (5), entitățile financiare mențin inventarele relevante și le actualizează periodic și de fiecare dată când are loc orice modificare majoră, astfel cum este menționată la alineatul (3).

(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 moștenite și, în orice caz, înainte și după conectarea tehnologiilor, aplicațiilor sau sistemelor.

*Articolul 9*

**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 securitatea și funcționarea sistemelor și a instrumentelor TIC și reduc la minimum impactul riscurilor TIC asupra sistemelor TIC prin utilizarea unor instrumente, politici și proceduri de securitate TIC adecvate.

(2) Entitățile financiare concep, achiziționează și pun în aplicare politici, proceduri, protocoale și instrumente în domeniul securității TIC care vizează să asigure reziliența, continuitatea și disponibilitatea sistemelor TIC, în special pentru cele care sprijină funcții critice sau importante, precum și să mențină standarde înalte de disponibilitate, autenticitate, integritate și confidențialitate a datelor, indiferent dacă sunt în repaus, în uz sau în tranzit.

(3) În vederea realizării obiectivelor menționate la alineatul (2), entitățile financiare utilizează soluții și procese TIC care sunt adecvate în conformitate cu articolul 4. Respectivele soluții și procese TIC:

(a) asigură securitatea mijloacelor de transfer al datelor;

(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) previn lipsa disponibilității, deteriorarea autenticității și a integrității, încălcarea confidențialității și pierderea datelor;

(d) asigură protecția datelor împotriva riscurilor care decurg din gestionarea datelor, inclusiv gestionarea deficitară, precum și împotriva riscurilor legate de prelucrare și a erorii umane.

(4) Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1), entitățile financiare:

(a) elaborează și documentează o politică de securitate a informațiilor care definește norme de protecție a disponibilității, autenticității, integrității și confidențialității datelor, a activelor informaționale și a activelor TIC, inclusiv a celor ale clienților lor, după caz;

(b) stabilesc, urmând o abordare bazată pe riscuri, o structură de gestionare solidă a rețelei și a infrastructurii care utilizează tehnici, metode și protocoale adecvate ce pot include 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 sau logic la activele informaționale și activele TIC la ceea ce este necesar exclusiv pentru funcții și activități legitime și aprobate și stabilesc în acest scop un set de politici, proceduri și controale care să vizeze drepturile de acces și o bună administrare a acestora;

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

(e) pun în aplicare politici, proceduri și controale documentate pentru gestionarea modificărilor la nivelul TIC, inclusiv modificări la nivelul componentelor software, hardware, firmware, parametrii sistemelor sau 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 documentate adecvate și cuprinzătoare pentru corecții și actualizări.

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

În scopul aplicării literei (e) de la primul paragraf, procesul de gestionare a modificărilor la nivelul TIC este aprobat de liniile de management corespunzătoare și dispune de protocoale specifice.

*Articolul 10*

**Detectare**

(1) Entitățile financiare dispun de mecanisme pentru detectarea rapidă a activităților anormale, în conformitate cu articolul 17, inclusiv a problemelor legate de performanța rețelei TIC și a incidentelor legate de TIC, precum și pentru identificarea posibilelor puncte unice de defecțiune semnificative.

Toate mecanismele de detectare menționate la primul paragraf sunt testate cu regularitate în conformitate cu articolul 25.

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

(3) Entitățile financiare alocă suficiente resurse și capacități pentru a monitoriza activitatea utilizatorilor, apariția anomaliilor TIC și a incidentelor legate de TIC, în special a atacurilor cibernetice.

(4) Furnizorii de servicii de raportare a datelor 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 rapoartelor respective.

*Articolul 11*

**Răspuns și recuperare**

(1) Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1) și pe baza cerințelor de identificare prevăzute la articolul 8, entitățile financiare instituie o politică cuprinzătoare de continuitate a activității TIC, care poate fi adoptată sub forma unei politici specifice dedicate, ca parte integrantă a politicii generale de continuitate a activității a entității financiare.

(2) Entitățile financiare pun în aplicare politica de continuitate a activității TIC prin măsuri, planuri, proceduri și mecanisme specifice, adecvate și documentate care vizează:

(a) asigurarea continuității funcțiilor critice sau importante ale entității financiare;

(b) un răspuns rapid, adecvat și eficace la toate incidentele legate de TIC și soluționarea tuturor acestor incidente, într-un mod care să limiteze daunele și să acorde prioritate reluării activităților și acțiunilor de recuperare;

(c) 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 previn producerea unor daune suplimentare, precum și a unor proceduri de răspuns și de recuperare adaptate, stabilite în conformitate cu articolul 12;

(d) estimarea efectelor, a daunelor și a pierderilor preliminare;

(e) 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 14, și raportarea către autoritățile competente, în conformitate cu articolul 19.

(3) Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1), entitățile financiare pun în aplicare planuri de răspuns și de recuperare în domeniul TIC asociate care, în cazul altor entități financiare decât microîntreprinderile, sunt supuse unor evaluări de audit intern independente.

(4) Entitățile financiare instituie, mențin și testează periodic planuri de continuitate a activității TIC adecvate, 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 politicii generale de continuitate a activității, entitățile financiare efectuează o analiză a impactului asupra activității (AIA) al expunerilor lor la perturbări grave ale activității. În conformitate cu AIA, entitățile financiare evaluează impactul potențial al perturbărilor grave ale activității cu ajutorul unor criterii cantitative și calitative, utilizând date interne și externe și analize de scenarii, după caz. AIA ia în considerare caracterul critic al funcțiilor operaționale identificate și cartografiate, al proceselor de sprijin, al dependențelor față de terți și al activelor informaționale, precum și interdependențele acestora. Entitățile financiare se asigură că activele TIC și serviciile TIC sunt proiectate și utilizate în deplină conformitate cu AIA, în special în ceea ce privește asigurarea în mod adecvat a redundanței tuturor componentelor critice.

(6) Ca parte a gestionării lor cuprinzătoare a riscurilor TIC, entitățile financiare:

(a) testează planurile de continuitate a activității TIC și planurile de răspuns și de recuperare în domeniul TIC în legătură cu sistemele TIC care sprijină toate funcțiile cel puțin o dată pe an, precum și în caz de eventuale modificări substanțiale ale sistemelor TIC care sprijină funcții critice sau importante;

(b) testează planurile de comunicare în situații de criză instituite în conformitate cu articolul 14.

În scopul aplicării literei (a) de la primul paragraf, entitățile financiare altele decât microîntreprinderile includ în planurile de testare scenarii de atacuri cibernetice și transferuri între infrastructura TIC primară și capacitățile redundante, copiile de rezervă și instalațiile redundante necesare pentru a îndeplini obligațiile prevăzute la articolul 12.

Entitățile financiare își revizuiesc periodic politica de continuitate a activității TIC și planurile de răspuns și de recuperare în domeniul TIC, ținând seama de rezultatele testelor efectuate în conformitate cu primul paragraf, precum și de recomandările care decurg din evaluările de audit sau procesele de supraveghere.

(7) Entitățile financiare altele decât microîntreprinderile au o funcție de gestionare a crizelor, care, în caz de activare a planurilor lor de continuitate a activității TIC sau a planurilor lor de răspuns și de recuperare în domeniul TIC, stabilește, printre altele, proceduri clare de gestionare a comunicărilor interne și externe în situații de criză, în conformitate cu articolul 14.

(8) Entitățile financiare păstrează o evidență ușor accesibilă a activităților înainte și în timpul evenimentelor perturbatoare atunci când sunt activate planurile lor de continuitate a activității TIC și planurile lor de răspuns și de recuperare în domeniul TIC.

(9) Depozitarii centrali de titluri de valoare furnizează autorităților competente copii ale rezultatelor testelor privind continuitatea activității TIC sau ale unor exerciții similare.

(10) Entitățile financiare, altele decât microîntreprinderile, raportează autorităților competente, la cererea acestora, o estimare a costurilor și a pierderilor anuale agregate cauzate de incidente majore legate de TIC.

(11) În conformitate cu articolul 16 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010, AES elaborează, prin intermediul Comitetului comun, până la 17 iulie 2024, orientări comune privind estimarea costurilor și pierderilor anuale agregate menționate la alineatul (10).

*Articolul 12*

**Politici și proceduri privind copiile de rezervă și proceduri și metode de restaurare și recuperare**

(1) Pentru a asigura restaurarea sistemelor TIC și a datelor cu o perioadă de indisponibilitate minimă și o perturbare și o pierdere limitate, ca parte a cadrului lor de gestionare a riscurilor TIC, entitățile financiare elaborează și documentează:

(a) politici și proceduri privind copiile de rezervă care precizează 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 al nivelului de confidențialitate al datelor;

(b) proceduri și metode de restaurare și recuperare.

(2) Entitățile financiare instituie sisteme de rezervă care pot fi activate în conformitate cu politicile și procedurile privind copiile de rezervă, precum și cu procedurile și metodele de restaurare și recuperare. Activarea sistemelor de rezervă nu pune în pericol securitatea rețelelor și a sistemelor informatice sau disponibilitatea, autenticitatea, integritatea ori confidențialitatea datelor. Periodic se efectuează testarea procedurilor privind copiile de rezervă și a procedurilor și metodelor de restaurare și recuperare.

(3) Atunci când restaurează date de rezervă pe baza sistemelor proprii, entitățile financiare utilizează sisteme TIC care sunt separate fizic și logic de sistemul TIC sursă. Sistemele TIC sunt securizate împotriva oricărui acces neautorizat sau a deteriorării TIC și permit restaurarea în timp util a serviciilor care utilizează copii de rezervă ale datelor și sistemelor, după caz.

În cazul contrapărților centrale, 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.

În plus, furnizorii de servicii de raportare a datelor mențin resurse adecvate și dispun de instalații pentru copii de rezervă și de restaurare, cu scopul de a-și oferi și a-și menține serviciile viabile în orice moment.

(4) Entitățile financiare, altele decât microîntreprinderile, mențin capacități TIC redundante dotate cu resurse, capacități și funcții care sunt adecvate pentru a acoperi nevoile operaționale. Microîntreprinderile evaluează necesitatea menținerii unor astfel de capacități TIC redundante pe baza profilului lor de risc.

(5) Depozitarii centrali de titluri de valoare mențin cel puțin o unitate de prelucrare secundară, dotată cu resurse adecvate, capacități, funcții și resurse umane 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 afectarea acesteia de către evenimentul care a afectat unitatea de prelucrare principală;

(b) este capabilă să asigure continuitatea funcțiilor critice sau importante în mod identic cu unitatea de prelucrare principală sau să furnizeze serviciile la nivelul 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 funcțiilor critice sau importante în cazul în care unitatea de prelucrare principală a devenit indisponibilă.

(6) Pentru a stabili obiectivele cu privire la intervalele de timp și momentele de la care se pot recupera datele în urma unei întreruperi și intervalele maxime de recuperare în urma unei întreruperi, pentru fiecare funcție, entitățile financiare iau în considerare dacă este vorba de o funcție critică sau importantă și impactul potențial global asupra eficienței pieței. Aceste obiective temporale asigură că, în scenarii extreme, nivelurile convenite ale serviciilor sunt respectate.

(7) În cazul recuperării în urma unui incident legat de TIC, entitățile financiare efectuează verificări necesare, inclusiv verificări și reconcilieri multiple, 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 13*

**Învățăminte și perspective de dezvoltare**

(1) Entitățile financiare dispun de capacități și de personal pentru a colecta informații cu privire la vulnerabilități, amenințări cibernetice și incidente legate de TIC, în special atacuri cibernetice, și pentru a analiza impactul pe care acestea l-ar putea avea asupra rezilienței lor operaționale digitale.

(2) Entitățile financiare instituie verificări ulterioare incidentelor legate de TIC după ce un incident major legat de TIC le perturbă activitățile de bază, analizând cauzele perturbării și identificând îmbunătățirile necesare pentru operațiunile TIC sau în cadrul politicii de continuitate a activității TIC menționate la articolul 11.

Entitățile financiare, altele decât microîntreprinderile, comunică autorităților competente, la cerere, modificările care au fost operate în urma verificărilor ulterioare incidentelor legate de TIC, astfel cum sunt menționate la primul paragraf.

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

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

(b) calitatea și rapiditatea efectuării unei analize judiciare, acolo unde se consideră necesar;

(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 rezilienței operaționale digitale, efectuată în conformitate cu articolele 26 și 27, precum și în urma incidentelor reale legate de TIC, în special a atacurilor cibernetice, alături de provocările întâmpinate la activarea planurilor de continuitate a activității TIC și a planurilor de răspuns și de recuperare în domeniul TIC, 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. Constatările respective stau la baza unor revizuiri corespunzătoare ale componentelor relevante ale cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1).

(4) Entitățile financiare monitorizează eficacitatea punerii în aplicare a strategiei lor privind reziliența operațională digitală menționate la articolul 6 alineatul (8). 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, în special în legătură cu funcțiile critice sau importante, 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 conștientizare 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. Respectivele programe și cursuri de formare se aplică tuturor angajaților și personalului de conducere de nivel superior și au un nivel de complexitate proporțional cu sfera de competență a funcțiilor lor. După caz, entitățile financiare includ, de asemenea, furnizorii terți de servicii TIC în programele lor de formare relevante, în conformitate cu articolul 30 alineatul (2) litera (i).

(7) Entitățile financiare altele decât microîntreprinderile 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 aibă informații actualizate cu privire la cele mai recente procese de gestionare a riscurilor TIC, cu scopul de a contracara cu eficacitate formele existente sau noi de atacuri cibernetice.

*Articolul 14*

**Comunicare**

(1) Ca parte a cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (1), entitățile financiare instituie planuri de comunicare în situații de criză care permit o informare responsabilă a clienților și a contrapărților, precum și a publicului, după caz, cu privire la, cel puțin, incidentele majore sau vulnerabilitățile legate de TIC.

(2) Ca parte a cadrului de gestionare a riscurilor TIC, entitățile financiare pun în aplicare politici de comunicare pentru personalul intern 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 personalul responsabil pentru răspuns și recuperare, și personalul care trebuie să fie informat.

(3) Cel puțin o persoană din entitatea financiară este însărcinată cu punerea în aplicare a strategiei de comunicare pentru incidentele legate de TIC și îndeplinește în acest scop funcția de legătură cu publicul și mass-media.

*Articolul 15*

**Armonizarea suplimentară a instrumentelor, metodelor, proceselor și politicilor de gestionare a riscurilor TIC**

AES elaborează, prin intermediul Comitetului comun, în consultare cu Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), proiecte comune de standarde tehnice de reglementare în următoarele scopuri:

(a) pentru a aduce precizări suplimentare privind elementele necesare a fi incluse în politicile, procedurile, protocoalele și instrumentele de securitate TIC menționate la articolul 9 alineatul (2), în scopul asigurării securității rețelelor, al asigurării unor garanții adecvate împotriva intruziunilor și a utilizării necorespunzătoare a datelor, al menținerii disponibilității, autenticității, integrității și confidențialității datelor, inclusiv tehnici criptografice, și al garantării unei transmiteri exacte și rapide a datelor fără perturbări majore și fără întârzieri nejustificate;

(b) pentru a aduce precizări suplimentare privind componentele controalelor drepturilor de gestionare a accesului menționate la articolul 9 alineatul (4) litera (c) și politica privind resursele umane aferentă, precizând 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;

(c) pentru a aduce precizări suplimentare privind mecanismele menționate la articolul 10 alineatul (1) care permit detectarea rapidă a activităților anormale și criteriile menționate la articolul 10 alineatul (2) care declanșează procesele de detectare și de răspuns la incidentele legate de TIC;

(d) pentru a aduce precizări suplimentare privind componentele politicii de continuitate a activității TIC, menționată la articolul 11 alineatul (1);

(e) pentru a aduce precizări suplimentare privind testarea planurilor de continuitate a activității TIC menționate la articolul 11 alineatul (6), pentru a asigura faptul că o astfel de testare 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;

(f) pentru a aduce precizări suplimentare privind componentele planurilor de răspuns și de recuperare în domeniul TIC menționate la articolul 11 alineatul (3);

(g) pentru a aduce precizări suplimentare privind conținutul și formatul raportului referitor la revizuirea cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (5).

Atunci când elaborează proiectele respective de standarde tehnice de reglementare, AES iau în considerare dimensiunea și profilul general de risc al entității financiare, precum și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor sale, ținând seama în mod corespunzător de orice caracteristică specifică care decurge din natura distinctă a activităților din diferite sectoare de servicii financiare.

AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 ianuarie 2024.

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. 1094/2010 și (UE) nr. 1095/2010.

*Articolul 16*

**Cadrul simplificat de gestionare a riscurilor TIC**

(1) Articolele 5-15 din prezentul regulament nu se aplică firmelor de investiții mici și neinterconectate, instituțiilor de plată exceptate în temeiul Directivei (UE) 2015/2366; instituțiilor exceptate în temeiul Directivei 2013/36/UE în cazul cărora statele membre au decis să nu aplice opțiunea menționată la articolul 2 alineatul (4) din prezentul regulament; instituțiilor emitente de monedă electronică exceptate în temeiul Directivei 2009/110/CE; și nici instituțiilor mici pentru furnizarea de pensii ocupaționale.

Fără a aduce atingere primului paragraf, entitățile menționate la primul paragraf:

(a) instituie și mențin un cadru solid și documentat de gestionare a riscurilor TIC care detaliază mecanismele și măsurile care vizează o gestionare rapidă, eficientă și cuprinzătoare a riscurilor TIC, inclusiv pentru protecția componentelor și infrastructurilor fizice relevante;

(b) monitorizează în permanență securitatea și funcționarea tuturor sistemelor TIC;

(c) reduc la minimum impactul riscurilor TIC prin utilizarea unor sisteme, protocoale și instrumente TIC solide, reziliente și actualizate care sunt adecvate pentru a sprijini desfășurarea activităților lor și furnizarea serviciilor și protejează în mod adecvat disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor din rețele și sistemele informatice;

(d) permit identificarea și detectarea rapidă a surselor de riscuri TIC și a anomaliilor din rețele și sistemele informatice, precum și gestionarea rapidă a incidentelor legate de TIC;

(e) identifică principalele dependențe față de furnizorii terți de servicii TIC;

(f) asigură continuitatea funcțiilor critice sau importante, prin planuri de continuitate a activității și măsuri de răspuns și de recuperare, care includ, cel puțin, măsuri privind copii de rezervă și restaurarea;

(g) testează cu regularitate planurile și măsurile menționate la litera (f), precum și eficacitatea controalelor puse în aplicare în conformitate cu literele (a) și (c);

(h) implementează, după caz, concluziile operaționale relevante rezultate din testele menționate la litera (g) și din analiza ulterioară incidentului în procesul de evaluare a riscurilor TIC și elaborează, în funcție de nevoi și de profilul de risc TIC, programe de conștientizare cu privire la securitatea TIC și cursuri de formare în domeniul rezilienței operaționale digitale destinate personalului și conducerii.

(2) Cadrul de gestionare a riscurilor TIC menționat la alineatul (1) al doilea paragraf litera (a) se documentează și se revizuiește periodic, precum și în momentul producerii unor incidente majore legate de TIC, în conformitate cu instrucțiunile de supraveghere. Acesta este îmbunătățit în permanență, pe baza învățămintelor desprinse în urma punerii în aplicare și a monitorizării. Autorității competente i se prezintă, la cererea sa, un raport privind revizuirea cadrului de gestionare a riscurilor TIC.

(3) AES elaborează, prin intermediul Comitetului comun, în consultare cu ENISA, proiecte comune de standarde tehnice de reglementare în următoarele scopuri:

(a) pentru a aduce precizări suplimentare privind elementele care trebuie incluse în cadrul de gestionare a riscurilor TIC menționat la alineatul (1) al doilea paragraf litera (a);

(b) pentru a aduce precizări suplimentare privind elementele legate de sistemele, protocoalele și instrumentele destinate reducerii la minimum a impactului riscurilor TIC menționate la alineatul (1) al doilea paragraf litera (c), în scopul asigurării securității rețelelor, al asigurării unor garanții adecvate împotriva intruziunilor și a utilizării necorespunzătoare a datelor și al menținerii disponibilității, autenticității, integrității și confidențialității datelor;

(c) pentru a aduce precizări suplimentare privind componentele planurilor de continuitate a activității TIC menționate la alineatul (1) al doilea paragraf litera (f);

(d) pentru a aduce precizări suplimentare privind normele referitoare la testarea planurilor de continuitate a activității și pentru a asigura eficacitatea controalelor menționate la alineatul (1) al doilea paragraf litera (g), precum și pentru a garanta faptul că o astfel de testare 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;

(e) pentru a aduce precizări suplimentare privind conținutul și formatul raportului referitor la revizuirea cadrului de gestionare a riscurilor TIC menționat la alineatul (2).

Atunci când elaborează proiectele respective de standarde tehnice de reglementare, AES iau în considerare dimensiunea și profilul general de risc al entității financiare, precum și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor sale.

AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 ianuarie 2024.

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. 1094/2010 și (UE) nr. 1095/2010.

*CAPITOLUL III*

## *Gestionarea, clasificarea și raportarea incidentelor legate de TIC*

*Articolul 17*

### Procesul de gestionare a incidentelor legate de TIC

(1) Entitățile financiare definesc, instituie 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.

(2) Entitățile financiare înregistrează toate incidentele legate de TIC și amenințările cibernetice semnificative. Entitățile financiare instituie proceduri și procese adecvate pentru a garanta monitorizarea, tratarea și urmărirea consecventă și integrată a incidentelor legate de TIC, pentru a asigura identificarea, documentarea și abordarea 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) instituie indicatori de avertizare timpurie;

(b) stabilește proceduri pentru identificarea, urmărirea, înregistrarea, indicarea categoriei și clasificarea incidentelor legate de TIC în funcție de prioritatea și de gravitatea lor și în funcție de caracterul critic al serviciilor afectate, în conformitate cu criteriile stabilite la articolul 18 alineatul (1);

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

(d) stabilește planuri pentru comunicarea cu personalul, cu părțile interesate externe și cu mass-media, în conformitate cu articolul 14, 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;

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

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

*Articolul 18*

**Clasificarea incidentelor legate de TIC și a amenințărilor cibernetice**

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

(a) numărul și/sau relevanța clienților sau a contrapărților financiare afectate și, după caz, cuantumul și numărul tranzacțiilor afectate de incidentul legat de TIC, precum și eventualul impact al incidentului legat de TIC 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 în cazul în care acesta afectează mai mult de două state membre;

(d) pierderile de date pe care le implică incidentul legat de TIC, în ceea ce privește disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor;

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

(f) impactul economic, în special costurile și pierderile directe și indirecte, ale incidentului legat de TIC, în termeni atât absoluți, cât și relativi.

(2) Entitățile financiare clasifică amenințările cibernetice ca fiind semnificative pe baza caracterului critic al serviciilor expuse riscului, inclusiv al tranzacțiilor și operațiunilor entității financiare, precum și pe baza numărului și/sau relevanței clienților sau a contrapărților financiare vizate și a întinderii geografice a zonelor expuse riscului.

(3) AES elaborează, prin intermediul Comitetului comun și în consultare cu BCE și ENISA, proiecte comune de standarde tehnice de reglementare pentru a aduce precizări suplimentare privind următoarele:

(a) criteriile menționate la alineatul (1), inclusiv pragurile de semnificație pentru determinarea incidentelor majore legate de TIC sau, după caz, a incidentelor majore operaționale sau de securitate legate de plăți care fac obiectul obligației de raportare prevăzute la articolul 19 alineatul (1);

(b) criteriile care trebuie aplicate de autoritățile competente în scopul evaluării relevanței incidentelor majore legate de TIC sau, după caz, a incidentelor majore operaționale sau de securitate legate de plăți, pentru autoritățile competente relevante ale altor state membre, precum și detaliile rapoartelor referitoare la incidentele majore legate de TIC sau, după caz, incidentele majore operaționale sau de securitate legate de plăți care trebuie să fie comunicate altor autorități competente în temeiul articolului 19 alineatele (6) și (7);

(c) criteriile prevăzute la alineatul (2) de la prezentul articol, inclusiv pragurile înalte de semnificație pentru determinarea amenințărilor cibernetice semnificative.

(4) Atunci când elaborează proiectele comune de standarde tehnice de reglementare menționate la alineatul (3) de la prezentul articol, AES țin seama de criteriile stabilite la articolul 4 alineatul (2), precum și de standardele internaționale și de orientările și specificațiile elaborate și publicate de ENISA, inclusiv, după caz, de specificațiile pentru alte sectoare economice. În scopul aplicării criteriilor prevăzute la articolul 4 alineatul (2), AES iau în considerare în mod corespunzător necesitatea ca microîntreprinderile și întreprinderile mici și mijlocii să mobilizeze resurse și capacități suficiente pentru a se asigura că incidentele legate de TIC sunt gestionate rapid.

AES transmit Comisiei aceste proiecte comune de standarde tehnice de reglementare până la 17 ianuarie 2024.

Se deleagă Comisiei competența de a completa prezentul regulament prin adoptarea standardelor tehnice de reglementare menționate la alineatul (3), în conformitate cu articolele 10-14 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010.

*Articolul 19*

**Raportarea incidentelor majore legate de TIC și notificarea voluntară a amenințărilor cibernetice semnificative**

(1) Entitățile financiare raportează incidentele majore legate de TIC autorității competente relevante menționate la articolul 46 în conformitate cu alineatul (4) de la prezentul articol.

În cazul în care o entitate financiară face obiectul supravegherii de către mai mult de o autoritate națională competentă astfel cum este menționată la articolul 46, statele membre desemnează o autoritate competentă unică drept autoritate competentă relevantă responsabilă cu îndeplinirea funcțiilor și a sarcinilor prevăzute la prezentul articol.

Instituțiile de credit clasificate drept semnificative, în conformitate cu articolul 6 alineatul (4) din Regulamentul (UE) nr. 1024/2013, prezintă un raport referitor la incidentele majore legate de TIC autorității naționale competente relevante desemnate în conformitate cu articolul 4 din Directiva 2013/36/UE, care transmite imediat raportul respectiv către BCE.

În sensul primului paragraf, după colectarea și analizarea tuturor informațiilor relevante, entitățile financiare efectuează notificarea inițială și elaborează rapoartele menționate la alineatul (4) de la prezentul articol, utilizând modelele menționate la articolul 20, și le transmit autorității competente. În cazul în care o imposibilitate tehnică împiedică transmiterea notificării inițiale utilizând modelul, entitățile financiare informează autoritatea competentă cu privire la aceasta prin mijloace alternative.

Notificarea inițială și rapoartele menționate la alineatul (4) includ toate informațiile necesare autorității competente pentru a determina semnificația incidentului major legat de TIC și a evalua posibilele efecte transfrontaliere.

Fără a aduce atingere raportării prevăzute la primul paragraf de către entitățile financiare către autoritatea competentă relevantă, statele membre pot stabili în plus ca unele entități financiare sau toate aceste entități să transmită, de asemenea, notificarea inițială și fiecare raport menționat la alineatul (4) de la prezentul articol, folosind modelele menționate la articolul 20, autorităților competente sau echipelor de intervenție în caz de incidente de securitate informatică (echipe CSIRT) desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555.

(2) Entitățile financiare pot notifica, în mod voluntar, amenințările cibernetice semnificative către autoritatea competentă relevantă atunci când consideră că amenințarea este relevantă pentru sistemul financiar, pentru utilizatorii serviciilor sau pentru clienți. Autoritatea competentă relevantă poate furniza astfel de informații și altor autorități relevante, menționate la alineatul (6).

Instituțiile de credit clasificate drept semnificative, în conformitate cu articolul 6 alineatul (4) din Regulamentul (UE) nr. 1024/2013, pot notifica, în mod voluntar, amenințările cibernetice semnificative către autoritatea națională competentă relevantă, desemnată în conformitate cu articolul 4 din Directiva 2013/36/UE, care transmite imediat notificarea către BCE.

Statele membre pot stabili că entitățile financiare care fac în mod voluntar o notificare în conformitate cu primul paragraf pot transmite, de asemenea, notificarea respectivă către echipele CSIRT desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555.

(3) În cazul în care are loc un incident major legat de TIC care are un impact asupra intereselor financiare ale clienților lor, entitățile financiare îi informează pe aceștia, fără întârzieri nejustificate, de îndată ce află despre incidentul major legat de TIC, cu privire la incidentul respectiv și la măsurile care au fost luate pentru a atenua efectele negative ale unui astfel de incident.

În cazul unei amenințări cibernetice semnificative, entitățile financiare își informează, după caz, clienții care ar putea fi afectați cu privire la eventualele măsuri de protecție adecvate pe care aceștia din urmă ar putea dori să le ia.

(4) Până la termenele care urmează să fie stabilite în conformitate cu articolul 20 primul paragraf litera (a) punctul (ii), entitățile financiare transmit autorității competente relevante următoarele:

(a) o notificare inițială;

(b) un raport intermediar după notificarea inițială menționată la litera (a) de îndată ce starea incidentului inițial s-a schimbat în mod semnificativ sau gestionarea incidentului major legat de TIC s-a schimbat pe baza noilor informații disponibile, urmat, după caz, de notificări actualizate de fiecare dată când este disponibilă o actualizare relevantă a stării, precum și la cererea 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.

(5) Entitățile financiare pot externaliza, în conformitate cu legislația sectorială a Uniunii și cu cea națională, obligațiile de raportare prevăzute la prezentul articol către un furnizor terț de servicii. În cazul unei astfel de externalizări, entitatea financiară rămâne pe deplin responsabilă de îndeplinirea cerințelor legate de raportarea incidentului.

(6) La primirea notificării inițiale și a fiecărui raport menționat la alineatul (4), autoritatea competentă furnizează, în timp util, detalii privind incidentul major legat de TIC următorilor destinatari, pe baza, după caz, a competențelor lor respective:

(a) ABE, ESMA sau EIOPA;

(b) BCE, în cazul entităților financiare menționate la articolul 2 alineatul (1) literele (a), (b) și (d);

(c) autoritățile competente, punctele unice de contact sau echipele CSIRT desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555;

(d) autoritățile de rezoluție, astfel cum sunt menționate la articolul 3 din Directiva 2014/59/UE, și Comitetul unic de rezoluție (SRB) în ceea ce privește entitățile menționate la articolul 7 alineatul (2) din Regulamentul (UE) nr. 806/2014 al Parlamentului European și al Consiliului ([37]), precum și în ceea ce privește entitățile și grupurile menționate la articolul 7 alineatul (4) litera (b) și alineatul (5) din Regulamentul (UE) nr. 806/2014 dacă aceste detalii se referă la incidente care prezintă un risc pentru asigurarea funcțiilor critice în sensul articolului 2 alineatul (1) punctul 35 din Directiva 2014/59/UE; și

(e) alte autorități publice relevante în temeiul dreptului intern.

(7) După primirea informațiilor în conformitate cu alineatul (6), ABE, ESMA sau EIOPA și BCE, în consultare cu ENISA și în cooperare cu autoritatea competentă relevantă, evaluează dacă incidentul major legat de TIC este relevant pentru autoritățile competente din alte state membre. În urma acestei evaluări, ABE, ESMA sau EIOPA notifică în consecință, cât mai curând posibil, autoritățile competente relevante din alte state membre. 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.

([37]) Regulamentul (UE) nr. 806/2014 al Parlamentului European și al Consiliului din 15 iulie 2014 de stabilire a unor norme uniforme și a unei proceduri uniforme de rezoluție a instituțiilor de credit și a anumitor firme de investiții în cadrul unui mecanism unic de rezoluție și al unui fond unic de rezoluție și de modificare a Regulamentului (UE) nr. 1093/2010 (JO L 225, 30.7.2014, p. 1).

(8) Notificarea care trebuie efectuată de ESMA în temeiul alineatului (7) de la prezentul articol nu aduce atingere responsabilității autorității competente de a transmite de urgență detaliile incidentului major legat de TIC autorității relevante din statul membru gazdă, în cazul în care un depozitar central de titluri de valoare desfășoară o activitate transfrontalieră semnificativă în statul membru gazdă, în cazul în care incidentul major legat de TIC este susceptibil să genereze consecințe grave pentru piețele financiare din statul membru gazdă și în cazul în care există acorduri de cooperare între autoritățile competente în ceea ce privește supravegherea entităților financiare.

*Articolul 20*

**Armonizarea conținutului rapoartelor și a modelelor de rapoarte**

AES, prin intermediul Comitetului comun și în consultare cu ENISA și BCE, elaborează:

(a) proiecte comune de standarde tehnice de reglementare având ca scop următoarele:

(i) stabilirea conținutului rapoartelor în cazul incidentelor majore legate de TIC, cu scopul de a reflecta criteriile prevăzute la articolul 18 alineatul (1) și de a include elemente suplimentare, precum detalii pentru a stabili dacă rapoartele sunt relevante pentru alte state membre și dacă incidentele constituie incidente majore operaționale sau de securitate legate de plăți;

(ii) stabilirea termenelor pentru notificarea inițială și pentru fiecare raport menționat la articolul 19 alineatul (4);

(iii) stabilirea conținutului notificării privind amenințările cibernetice semnificative.

Atunci când elaborează proiectele respective de standarde tehnice de reglementare, AES iau în considerare dimensiunea și profilul general de risc al entității financiare, precum și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor sale, în special pentru a se asigura că, în sensul literei (a) punctul (ii) de la prezentul paragraf, existența unor termene diferite poate reflecta, după caz, particularitățile sectoarelor financiare, fără a aduce atingere menținerii unei abordări coerente a raportării incidentelor legate de TIC în temeiul prezentului regulament și al Directivei (UE) 2022/2555. AES furnizează, după caz, justificări atunci când se abat de la abordările adoptate în contextul directivei respective;

(b) proiecte comune de standarde tehnice de punere în aplicare având ca scop stabilirea formularelor, modelelor și procedurilor standard pentru raportarea de către entitățile financiare a unui incident major legat de TIC și notificarea de către acestea a unei amenințări cibernetice semnificative.

AES transmit Comisiei proiectele comune de standarde tehnice de reglementare menționate la primul paragraf litera (a) și proiectele comune de standarde tehnice de punere în aplicare menționate la primul paragraf litera (b), până la 17 iulie 2024.

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

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

*Articolul 21*

**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 suplimentare a raportării incidentelor prin crearea unei platforme unice la nivelul UE pentru raportarea incidentelor majore legate de TIC de către entitățile financiare. Raportul comun 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 comun menționat la alineatul (1) cuprinde cel puțin următoarele elemente:

(a) condițiile prealabile pentru instituirea unei platforme unice la nivelul UE;

(b) beneficiile, limitările și riscurile, inclusiv riscurile asociate concentrării ridicate a informațiilor sensibile;

(c) capacitatea necesară pentru a asigura interoperabilitatea cu alte sisteme de raportare relevante;

(d) elemente ale gestionării operaționale;

(e) condițiile de participare;

(f) modalitățile tehnice de accesare a platformei unice la nivelul UE de către entitățile financiare și autoritățile naționale competente;

(g) o evaluare preliminară a costurilor suportate cu instituirea platformei operaționale care sprijină platforma unică la nivelul UE, inclusiv expertiza necesară.

(3) AES transmit raportul menționat la alineatul (1) Parlamentului European, Consiliului și Comisiei până la 17 ianuarie 2025.

*Articolul 22*

**Feedback privind supravegherea**

(1) Fără a aduce atingere contribuției, consultanței sau soluțiilor tehnice și urmăririi ulterioare care pot fi oferite, după caz, în conformitate cu dreptul intern, de către echipele CSIRT în temeiul Directivei (UE) 2022/2555, autoritatea competentă, la primirea notificării inițiale și a fiecărui raport menționate la articolul 19 alineatul (4), confirmă primirea și poate furniza autorității financiare, acolo unde este posibil, în timp util, feedback relevant și proporțional sau îndrumări la nivel înalt, în special prin punerea la dispoziție a oricăror informații și date operative relevante anonimizate cu privire la amenințări similare și poate discuta măsurile de remediere aplicate la nivelul entității financiare și modalități de reducere la minimum și de atenuare a impactului negativ la nivelul sectorului financiar. Fără a aduce atingere feedbackului privind supravegherea primit, entitățile financiare rămân pe deplin responsabile de gestionarea incidentelor legate de TIC raportate în temeiul articolului 19 alineatul (1) și de consecințele acestora.

(2) Prin intermediul Comitetului comun, AES raportează anual, în mod anonim și agregat, cu privire la incidentele majore legate de TIC, ale căror detalii sunt furnizate de autoritățile competente în conformitate cu articolul 19 alineatul (6), menționând cel puțin numărul incidentelor majore legate de TIC, natura acestora și impactul lor asupra operațiunilor entităților financiare sau ale clienților, măsurile de remediere luate și costurile suportate.

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

*Articolul 23*

**Incidente operaționale sau de securitate legate de plăți care vizează instituții de credit, instituții de plată, prestatori de servicii de informare cu privire la conturi și instituții emitente de monedă electronică**

Cerințele prevăzute în prezentul capitol se aplică, de asemenea, incidentelor operaționale sau de securitate legate de plăți și incidentelor operaționale sau de securitate majore legate de plăți, atunci când acestea vizează instituții de credit, instituții de plată, prestatori de servicii de informare cu privire la conturi și instituții emitente de monedă electronică.

*CAPITOLUL IV*

## *Testarea rezilienței operaționale digitale*

*Articolul 24*

### Cerințe generale pentru efectuarea testării rezilienței operaționale digitale

(1) În scopul evaluării nivelului de pregătire pentru gestionarea incidentelor legate de TIC, al identificării punctelor slabe, a deficiențelor și a lacunelor în ceea ce privește reziliența operațională digitală și al punerii în aplicare prompte a măsurilor corective, entitățile financiare, altele decât microîntreprinderile, stabilesc, mențin și revizuiesc, ținând seama de criteriile prevăzute la articolul 4 alineatul (2), un program solid și cuprinzător de testare a rezilienței operaționale digitale ca parte integrantă a cadrului de gestionare a riscurilor TIC menționat la articolul 6.

(2) Programul de testare a rezilienței operaționale digitale include o serie de evaluări, teste, metodologii, practici și instrumente care trebuie aplicate în conformitate cu articolele 25 și 26.

(3) Atunci când desfășoară programul de testare a rezilienței operaționale digitale menționat la alineatul (1) de la prezentul articol, entitățile financiare, altele decât microîntreprinderile, urmează o abordare bazată pe riscuri, ținând seama de criteriile prevăzute la articolul 4 alineatul (2) și luând în considerare în mod corespunzător evoluția peisajului riscurilor TIC, orice riscuri specifice la care entitatea financiară în cauză este sau ar putea fi expusă, caracterul critic al activelor informaționale și al serviciilor furnizate, precum și orice alt factor pe care entitatea financiară îl consideră adecvat.

(4) Entitățile financiare, altele decât microîntreprinderile, se asigură că testele sunt efectuate de părți independente, indiferent dacă sunt interne sau externe. Atunci când testele sunt efectuate de o entitate internă, entitățile financiare alocă resurse suficiente și se asigură că sunt evitate conflictele de interese pe parcursul fazelor de proiectare și execuție ale testului.

(5) Entitățile financiare, altele decât întreprinderile, stabilesc proceduri și politici care să prioritizeze, să clasifice și să remedieze toate chestiunile identificate 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, altele decât microîntreprinderile, se asigură că se efectuează teste adecvate cel puțin o dată pe an asupra tuturor sistemelor și aplicațiilor TIC care sprijină funcții critice sau importante.

*Articolul 25*

### Testarea instrumentelor și sistemelor TIC

(1) Programul de testare a rezilienței operaționale digitale menționat la articolul 24 asigură, în conformitate cu criteriile prevăzute la articolul 4 alineatul (2), efectuarea de teste adecvate, precum evaluări și examinări ale vulnerabilității, analize ale surselor deschise, evaluări ale securității rețelei, analize ale lacunelor, verificări ale securității fizice, chestionare și soluții de analiză de tip software, evaluări ale codului sursă acolo unde este posibil, teste bazate pe scenarii, teste de compatibilitate, teste de performanță, teste de la un capăt la altul (end-to-end) sau teste de penetrare.

(2) Depozitarii centrali de titluri de valoare și contrapărțile centrale efectuează evaluări ale vulnerabilității înainte de utilizarea sau reutilizarea unor aplicații și componente de infrastructură noi sau existente și servicii TIC care sprijină funcții critice sau importante ale entității financiare.

(3) Microîntreprinderile efectuează testele menționate la alineatul (1) combinând o abordare bazată pe riscuri cu o planificare strategică a testării TIC și luând în considerare în mod corespunzător necesitatea de a menține o abordare echilibrată între amploarea resurselor și timpul care urmează să fie alocat testării TIC prevăzute la prezentul articol, pe de o parte, și urgența, tipul de risc, caracterul critic al activelor informaționale și al serviciilor furnizate, precum și orice alt factor relevant, inclusiv capacitatea entității financiare de a-și asuma riscuri calculate, pe de altă parte.

*Articolul 26*

**Testarea avansată a instrumentelor, sistemelor și proceselor TIC cu ajutorul TLPT**

(1) Entitățile financiare, altele decât entitățile menționate la articolul 16 alineatul (1) primul paragraf și altele decât microîntreprinderile, care sunt identificate în conformitate cu alineatul (8) al treilea paragraf de la prezentul articol, efectuează, cel puțin o dată la trei ani, testări avansate prin intermediul TLPT. Pe baza profilului de risc al entității financiare și ținând seama de circumstanțele operaționale, autoritatea competentă poate să solicite entității financiare, dacă este necesar, să reducă sau să mărească această frecvență.

(2) Fiecare test de penetrare bazat pe amenințări acoperă unele sau toate funcțiile critice sau importante ale unei entități financiare și este realizat pe sistemele de producție în timp real care sprijină astfel de funcții.

Entitățile financiare identifică toate sistemele, procesele și tehnologiile TIC subiacente relevante care sprijină funcțiile critice sau importante și serviciile TIC, inclusiv pe cele care sprijină funcțiile critice sau importante care au fost externalizate sau contractate unor furnizori terți de servicii TIC.

Entitățile financiare evaluează ce funcții critice sau importante trebuie să fie acoperite de TLPT. Rezultatul acestei evaluări determină sfera de aplicare exactă a TLPT și este validat de autoritățile competente.

(3) În cazul în care furnizorii terți de servicii TIC sunt incluși în sfera de aplicare a TLPT, entitatea financiară ia măsurile și garanțiile necesare pentru a asigura participarea acestor furnizori terți de servicii TIC la TLPT și rămân în orice moment pe deplin responsabile de asigurarea respectării prezentului regulament.

(4) Fără a aduce atingere primului și celui de al doilea paragraf de la alineatul (2), în cazul în care se preconizează în mod rezonabil că participarea unui furnizor terț de servicii TIC la TLPT, astfel cum se menționează la alineatul (3), va avea un impact negativ asupra calității sau securității serviciilor oferite de către furnizorul terț de servicii TIC către clienți care sunt entități ce nu intră în domeniul de aplicare al prezentului regulament, sau asupra confidențialității datelor legate de astfel de servicii, entitatea financiară și furnizorul terț de servicii TIC pot conveni în scris ca furnizorul terț de servicii TIC să încheie în mod direct acorduri contractuale cu o entitate externă de testare în scopul desfășurării, sub conducerea unei entități financiare desemnate unice, a unei TLPT grupate, în care să fie implicate mai multe entități financiare (testare grupată) pentru care furnizorul terț de servicii TIC oferă servicii TIC.

Testarea grupată respectivă acoperă gama relevantă de servicii TIC care sprijină funcțiile critice sau importante contractate de către entitățile financiare respectivului furnizor terț de servicii TIC. Testarea grupată este considerată TLPT efectuată de entitățile financiare care participă la testarea grupată.

Numărul entităților financiare care participă la testarea grupată este calibrat în mod corespunzător, ținând seama de complexitatea și de tipurile serviciilor implicate.

(5) Entitățile financiare efectuează, cu cooperarea furnizorilor terți de servicii TIC și a altor părți implicate, inclusiv a entităților de testare, dar excluzând autoritățile competente, controale eficace ale gestionării riscurilor pentru a atenua riscurile unui potențial impact asupra datelor și riscurile de deteriorare a activelor și de perturbare a funcțiilor, a serviciilor sau a operațiunilor critice sau importante la nivelul entității financiare înseși, al contrapărților acesteia sau al sectorului financiar.

(6) La sfârșitul testării, după ce s-a convenit cu privire la rapoarte și la planurile de remediere, entitatea financiară și, după caz, entitățile externe de testare furnizează autorității desemnate în conformitate cu alineatul (9) sau (10) un rezumat al constatărilor relevante, planurile de remediere și documentația care demonstrează că TLPT a fost efectuată în conformitate cu cerințele.

(7) Autoritățile furnizează entităților financiare o adeverință prin care se confirmă faptul că testul a fost efectuat în conformitate cu cerințele evidențiate în documentație, pentru a permite recunoașterea reciprocă între autoritățile competente a testelor de penetrare bazate pe amenințări. Entitatea financiară notifică autorității competente relevante adeverința, rezumatul constatărilor relevante și planurile de remediere.

Fără a aduce atingere unei astfel de adeverințe, entitățile financiare rămân în orice moment pe deplin responsabile pentru impactul testelor menționate la alineatul (4).

(8) Entitățile financiare contractează entități de testare în scopul efectuării TLPT în conformitate cu articolul 27. Atunci când entitățile financiare utilizează entități interne de testare în scopul efectuării TLPT, acestea contractează entități externe de testare la fiecare trei teste.

Instituțiile de credit care sunt clasificate drept semnificative în conformitate cu articolul 6 alineatul (4) din Regulamentul (UE) nr. 1024/2013, utilizează numai entități externe de testare în conformitate cu articolul 27 alineatul (1) literele (a)-(e).

Autoritățile competente identifică entitățile financiare care sunt obligate să efectueze TLPT ținând seama de criteriile prevăzute la articolul 4 alineatul (2), pe baza unei evaluări a următoarelor elemente:

(a) factorii legați de impact, în special măsura în care serviciile furnizate și activitățile întreprinse de entitatea financiară au impact asupra sectorului financiar;

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

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

(9) Statele membre pot desemna o autoritate publică unică în sectorul financiar care să fie responsabilă de aspectele legate de TLPT în sectorul financiar la nivel național și îi încredințează acesteia toate competențele și sarcinile în acest sens.

(10) În absența unei desemnări în conformitate cu alineatul (9) de la prezentul articol și fără a aduce atingere competenței de a identifica entitățile financiare care trebuie să efectueze TLPT, o autoritate competentă poate delega exercitarea unora sau a tuturor sarcinilor menționate la prezentul articol și la articolul 27 unei alte autorități naționale din sectorul financiar.

(11) AES elaborează, în acord cu BCE, proiecte comune de standarde tehnice de reglementare în conformitate cu cadrul TIBER–EU pentru a aduce precizări suplimentare privind:

(a) criteriile utilizate în scopul aplicării alineatului (8) al doilea paragraf;

(b) cerințele și standardele care reglementează utilizarea entităților interne de testare;

(c) cerințele privind:

  (i) sfera de aplicare a TLPT menționată la alineatul (2);

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

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

(d) tipul de cooperare în materie de supraveghere și alt tip de cooperare relevant care sunt necesare pentru punerea în aplicare a TLPT și pentru facilitarea recunoașterii reciproce a testării respective, 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.

Atunci când elaborează proiectele respective de standarde tehnice de reglementare, AES țin seama în mod corespunzător de orice caracteristică specifică care decurge din natura distinctă a activităților din diferite sectoare de servicii financiare.

AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 iulie 2024.

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. 1094/2010 și (UE) nr. 1095/2010.

*Articolul 27*

**Cerințe pentru entitățile de testare în ceea ce privește efectuarea TLPT**

(1) Entitățile financiare utilizează, în scopul efectuării TLPT, numai entități de testare 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 și testarea de tipul „echipa roșie";

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

(d) oferă o asigurare independentă sau un raport de audit în ceea ce privește gestionarea solidă a riscurilor asociate cu efectuarea TLPT, inclusiv protecția corespunzătoare a informațiilor confidențiale ale entității financiare și măsurile reparatorii pentru riscurile legate de activitățile entității financiare;

(e) sunt acoperite în mod corespunzător și în totalitate de asigurările de răspundere civilă profesională relevante, inclusiv împotriva riscurilor de abatere și neglijență.

(2) În cazul utilizării entităților interne de testare, entitățile financiare se asigură că, în plus față de cerințele de la alineatul (1), se respectă toate condițiile următoare:

(a) utilizarea a fost aprobată de autoritatea competentă relevantă sau de autoritatea publică unică desemnată în conformitate cu articolul 26 alineatele (9) și (10);

(b) autoritatea competentă relevantă a verificat că entitatea financiară are suficiente resurse alocate și s-a asigurat că sunt evitate conflictele de interese pe parcursul fazelor de proiectare și execuție ale testului; și

(c) furnizorul de date operative privind amenințările este extern entității financiare.

(3) Entitățile financiare se asigură că contractele încheiate cu entități externe de testare impun o gestionare solidă a rezultatelor TLPT și că orice prelucrare de date de către acestea, inclusiv orice generare, stocare, agregare, elaborare, 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 28*

**Principii generale**

(1) Entitățile financiare gestionează riscurile TIC generate de părți terțe ca parte integrantă a riscurilor TIC în cadrul lor de gestionare a riscurilor TIC astfel cum este menționat la articolul 6 alineatul (1) și în conformitate cu următoarele principii:

(a) 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 dreptul aplicabil în domeniul serviciilor financiare;

(b) gestionarea de către entitățile financiare a riscurilor TIC generate de părți terțe este pusă în aplicare din perspectiva principiului proporționalității, luând în considerare:

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

(ii) 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 disponibilității serviciilor și activităților financiare, la nivel individual și la nivel de grup.

(2) Ca parte a cadrului lor de gestionare a riscurilor TIC, entitățile financiare, altele decât entitățile menționate la articolul 16 alineatul (1) primul paragraf și altele decât microîntreprinderile, adoptă și revizuiesc periodic o strategie privind riscurile TIC generate de părți terțe, ținând seama de strategia privind existența mai multor furnizori menționată la articolul 6 alineatul (9), după caz. Această strategie privind riscurile TIC generate de părți terțe include o politică privind utilizarea serviciilor TIC care sprijină funcții critice sau importante oferite de furnizori terți de servicii TIC și se aplică pe o bază individuală și, după caz, pe o bază subconsolidată și consolidată. Pe baza unei evaluări a profilului general de risc al entității financiare și a amplorii și complexității serviciilor comerciale, organul de conducere examinează periodic riscurile identificate în ceea ce privește acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante.

(3) 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 oferite de furnizori terți de servicii TIC.

Acordurile contractuale menționate la primul paragraf sunt documentate în mod corespunzător, făcându-se distincția între cele care acoperă servicii TIC de sprijinire a funcțiilor critice sau importante și cele care nu le acoperă.

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

Entitățile financiare pun la dispoziția autorității competente, la cererea acesteia, 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 orice acord contractual planificat privind utilizarea unor servicii TIC care sprijină funcții critice sau importante, precum și atunci când o funcție a devenit critică sau importantă.

(4) Înainte de a încheia un acord contractual privind utilizarea serviciilor TIC, entitățile financiare:

(a) evaluează dacă acordul contractual vizează utilizarea unor servicii TIC care sprijină 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 un astfel de acord contractual să contribuie la consolidarea riscului de concentrare a serviciilor TIC, astfel cum este menționat la articolul 29;

(d) efectuează toate diligențele necesare cu privire la potențialii furnizori terți de servicii TIC și se 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.

(5) Entitățile financiare pot încheia acorduri contractuale numai cu furnizori terți de servicii TIC care respectă standarde adecvate de securitate a informațiilor. În cazul în care acordurile contractuale respective se referă la funcții critice sau importante, entitățile financiare, înainte de încheierea acordurilor, țin seama în mod corespunzător de utilizarea de către furnizorii terți de servicii TIC a celor mai recente și de cea mai înaltă calitate standarde de securitate a informațiilor.

(6) 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 în care acordurile contractuale încheiate cu furnizori terți de servicii TIC privind utilizarea unor servicii TIC prezintă o complexitate tehnică ridicată, entitatea financiară verifică dacă auditorii, atât cei interni, cât și cei externi, sau un grup de auditori, dețin competențele și cunoștințele corespunzătoare pentru a efectua în mod eficace auditurile și evaluările relevante.

(7) Entitățile financiare se asigură că acordurile contractuale privind utilizarea serviciilor TIC pot fi reziliate în oricare dintre următoarele circumstanțe:

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

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

(c) deficiențe demonstrate ale furnizorului terț de servicii TIC legate de gestionarea sa generală a riscurilor TIC și, în special, legate de modul în care asigură disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor, fie date cu caracter personal sau date sensibile din alt punct de vedere, ori a datelor fără caracter personal;

(d) în cazul în care autoritatea competentă nu mai poate supraveghea în mod eficace entitatea financiară ca urmare a condițiilor acordului contractual respectiv sau a unor circumstanțe legate de acesta.

(8) Pentru serviciile TIC care sprijină funcții critice sau importante, entitățile financiare instituie strategii de ieșire. Strategiile de ieșire țin seama de riscurile care pot apărea la nivelul furnizorilor terți de servicii TIC, în special o posibilă deficiență din partea acestora, o deteriorare a calității serviciilor TIC oferite, orice perturbare a activității cauzată de furnizarea necorespunzătoare sau defectuoasă a serviciilor TIC sau orice riscuri semnificative care decurg din utilizarea adecvată și continuă a serviciului TIC respectiv ori încetarea acordurilor contractuale cu furnizorii terți de servicii TIC în oricare dintre situațiile enumerate la alineatul (7).

Entitățile financiare se asigură că pot să se retragă din acordurile contractuale fără:

(a) perturbarea activităților lor comerciale;

(b) limitarea respectării cerințelor în materie de reglementare;

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

Planurile de ieșire trebuie să fie cuprinzătoare, documentate și, în conformitate cu criteriile stabilite la articolul 4 alineatul (2), trebuie să fie testate în mod suficient și revizuite periodic.

Entitățile financiare identifică soluții alternative și dezvoltă planuri de tranziție care să le permită să elimine serviciile TIC 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 instituie măsuri adecvate pentru situații neprevăzute astfel încât să păstreze continuitatea activității în cazul apariției situațiilor menționate la primul paragraf.

(9) 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 (3), inclusiv informații care sunt comune tuturor acordurilor contractuale privind utilizarea serviciilor TIC. AES transmit Comisiei aceste proiecte de standarde tehnice de punere în aplicare până la 17 ianuarie 2024.

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. 1094/2010 și (UE) nr. 1095/2010.

(10) AES elaborează, prin intermediul Comitetului comun, proiecte de standarde tehnice de reglementare pentru a aduce precizări suplimentare privind conținutul detaliat al politicii menționate la alineatul (2) în legătură cu acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante oferite de furnizori terți de servicii TIC.

Atunci când elaborează proiectele respective de standarde tehnice de reglementare, AES iau în considerare dimensiunea și profilul general de risc al entității financiare, precum și natura, amploarea și complexitatea serviciilor, activităților și operațiunilor sale. AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 ianuarie 2024.

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. 1094/2010 și (UE) nr. 1095/2010.

*Articolul 29*

**Evaluarea preliminară a riscului de concentrare a serviciilor TIC**

(1) La identificarea și evaluarea riscurilor menționate la articolul 28 alineatul (4) litera (c), entitățile financiare iau în considerare, de asemenea, dacă încheierea preconizată a unui acord contractual în legătură cu servicii TIC care sprijină funcții critice sau importante ar conduce la oricare dintre următoarele situații:

(a) stabilirea unei relații contractuale 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 care sprijină funcții critice sau importante cu același furnizor terț de servicii TIC sau cu furnizori terți de servicii TIC strâns conectați.

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 acordurile contractuale privind utilizarea de servicii TIC care sprijină funcții critice sau importante includ posibilitatea ca un furnizor terț de servicii TIC să subcontracteze în continuare servicii TIC care sprijină 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 subcontractare, în special în cazul unui subcontractant TIC stabilit într-o țară terță.

În cazul în care acordurile contractuale privesc servicii TIC care sprijină funcții critice sau importante, entitățile financiare iau în considerare în mod corespunzător dispozițiile din legislația privind insolvența care s-ar aplica în eventualitatea falimentului furnizorului terț de servicii TIC, precum și orice constrângere care ar putea apărea în legătură cu recuperarea urgentă a datelor entității financiare.

Atunci când acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante sunt încheiate cu un furnizor terț de servicii TIC stabilit într-o țară terță, entitățile financiare iau în considerare, în afară de aspectele menționate la al doilea paragraf, și conformitatea cu normele Uniunii privind protecția datelor și asigurarea efectivă a respectării legii în respectiva țară terță.

Atunci când acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante prevăd subcontractarea, entitățile financiare evaluează dacă și în ce mod lanțurile de subcontractare potențial lungi sau complexe 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 30*

**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 include acordurile privind nivelul serviciilor **și** este consemnat într-un document scris care se află la dispoziția părților pe suport de hârtie sau într-un document având un alt format durabil, accesibil și care poate fi descărcat.

(2) Acordurile contractuale privind utilizarea serviciilor TIC includ cel puțin următoarele elemente:

(a) o descriere clară și completă a tuturor funcțiilor și serviciilor TIC care urmează să fie furnizate de furnizorul terț de servicii TIC, indicând dacă este permisă subcontractarea unui serviciu TIC care sprijină o funcție critică sau importantă sau părți semnificative ale acesteia și, în caz afirmativ, condițiile aplicabile acestei subcontractări;

(b) locurile, și anume regiunile sau țările, în care urmează să fie furnizate funcțiile și serviciile TIC 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 în prealabil entitatea financiară în cazul în care are în vedere modificarea acestor locuri;

(c) dispoziții privind disponibilitatea, autenticitatea, integritatea și confidențialitatea în ceea ce privește protecția datelor, inclusiv a datelor cu caracter personal;

(d) dispoziții privind 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 încetare a activității furnizorului terț de servicii TIC sau în cazul încetării acordurilor contractuale;

(e) descrieri la nivelul serviciilor, inclusiv actualizări și revizuiri ale acestora;

(f) obligația furnizorului terț de servicii TIC de a oferi asistență entității financiare fără costuri suplimentare sau la un cost stabilit ex ante, atunci când survine un incident TIC care este legat de serviciul TIC furnizat entității financiare;

(g) 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;

(h) drepturile de încetare și perioadele minime de preaviz aferente pentru încetarea acordurilor contractuale, în conformitate cu așteptările autorităților competente și ale autorităților de rezoluție;

(i) condițiile pentru participarea furnizorilor terți de servicii TIC la programele de conștientizare cu privire la securitatea TIC ale entităților financiare și la cursurile de formare în domeniul rezilienței operaționale digitale în conformitate cu articolul 13 alineatul (6).

(3) Acordurile contractuale privind utilizarea serviciilor TIC care sprijină funcții critice sau importante includ, în plus față de elementele menționate la alineatul (2), cel puțin următoarele:

(a) descrieri complete la nivelul serviciilor, inclusiv actualizări și revizuiri ale acestora, cu obiective cantitative și calitative precise privind performanța în limitele nivelurilor convenite ale serviciilor, pentru a permite monitorizarea eficace de către entitatea financiară a serviciilor TIC și adoptarea unor măsuri corective adecvate, fără întârzieri nejustificate, atunci când nu sunt asigurate nivelurile convenite ale serviciilor;

(b) 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 furniza în mod eficace serviciile TIC în sprijinul funcțiilor critice sau importante, în concordanță cu nivelurile convenite ale serviciului;

(c) 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 asigure un nivel adecvat de securitate în ceea ce privește furnizarea serviciilor de către entitatea financiară, în concordanță cu cadrul său de reglementare;

(d) obligația furnizorului terț de servicii TIC de a participa la TLPT ale entității financiare și de a coopera pe deplin în cadrul realizării acestora, astfel cum se menționează la articolele 26 și 27;

(e) dreptul de a monitoriza, în permanență, performanța furnizorului terț de servicii TIC, care presupune următoarele:

(i) drepturile nerestricționate de acces, de inspecție și de audit de către entitatea financiară sau o parte terță desemnată și de către autoritatea competentă, precum și dreptul de a produce copii ale documentelor relevante la fața locului, dacă acestea sunt esențiale pentru operațiunile furnizorului terț de servicii TIC, drepturi 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) obligația furnizorului terț de servicii TIC de a coopera pe deplin în timpul inspecțiilor și auditurilor la fața locului efectuate de autoritățile competente, de supraveghetorul principal, de entitatea financiară sau de o parte terță desemnată; și

(iv) obligația de a transmite detalii privind domeniul de aplicare, procedurile care trebuie urmate și frecvența unor astfel de inspecții și audituri;

(f) strategiile de ieșire, în special stabilirea unei perioade de tranziție adecvate obligatorii:

(i) în cursul căreia furnizorul terț de servicii TIC va continua să furnizeze funcțiile sau serviciile TIC respective vizând să reducă riscul de perturbare în cadrul entității financiare sau să asigure rezoluția și restructurarea sa eficace;

(ii) care permite entității financiare să migreze către un alt furnizor terț de servicii TIC sau să treacă la soluții dezvoltate de aceasta pe plan intern, în conformitate cu complexitatea serviciului furnizat.

Prin derogare de la litera (e), furnizorul terț de servicii TIC și entitatea financiară care este o microîntreprindere pot conveni ca drepturile de acces, de inspecție și de audit ale entității financiare să poată fi delegate unui terț independent, numit de furnizorul terț de servicii TIC, și ca entitatea financiară să poată solicita în orice moment din partea terțului informații și asigurări cu privire la performanța furnizorului terț de servicii TIC.

(4) La negocierea acordurilor contractuale, entitățile financiare și furnizorii terți de servicii TIC țin seama de utilizarea clauzelor contractuale standard elaborate de autoritățile publice pentru servicii specifice.

(5) AES elaborează, prin intermediul Comitetului comun, proiecte de standarde tehnice de reglementare pentru a aduce precizări suplimentare cu privire la elementele menționate la alineatul (2) litera (a), pe care o entitate financiară trebuie să le stabilească și să le evalueze atunci când subcontractează servicii TIC care sprijină funcții critice sau importante.

Atunci când elaborează aceste proiecte de standarde tehnice de reglementare, AES țin seama de dimensiunea și de profilul general de risc al entității financiare, precum și de natura, amploarea și complexitatea serviciilor, activităților și operațiunilor sale.

AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 iulie 2024.

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. 1094/2010 și (UE) nr. 1095/2010.

Secțiunea II

## Cadrul de supraveghere a furnizorilor terți esențiali de servicii TIC

*Articolul 31*

### Desemnarea furnizorilor terți esențiali de servicii TIC

(1) AES, prin intermediul Comitetului comun și la recomandarea Forumului de supraveghere instituit în temeiul articolului 32 alineatul (1):

(a) desemnează furnizorii terți de servicii TIC care sunt esențiali pentru entitățile financiare, în urma unei evaluări care ține seama de criteriile menționate la alineatul (2);

(b) desemnează drept supraveghetor principal pentru fiecare furnizor terț esențial de servicii TIC acea AES care este responsabilă, în conformitate cu Regulamentul (UE) nr. 1093/2010, (UE) nr. 1094/2010 sau (UE) nr. 1095/2010, de entitățile financiare care dețin împreună cea mai mare parte a activelor totale din valoarea activelor totale ale tuturor entităților financiare care utilizează serviciile furnizorului terț esențial de servicii TIC relevant, astfel cum reiese din suma bilanțurilor individuale ale entităților financiare respective.

(2) Desemnarea prevăzută la alineatul (1) litera (a) se bazează pe toate criteriile următoare în ceea ce privește serviciile TIC furnizate de furnizorul terț de servicii TIC:

(a) impactul sistemic asupra stabilității, continuității sau calității furnizării serviciilor financiare în situația în care furnizorul terț de servicii TIC relevant s-ar confrunta cu o defecțiune operațională la scară largă în ceea ce privește furnizarea serviciilor sale, ținând seama de numărul de entități financiare și de valoarea totală a activelor entităților 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 parțiale, 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 protejată, sau caracteristicile specifice ale modului de organizare sau ale activității furnizorului terț de servicii TIC;

(ii) dificultăți în ceea ce privește migrarea parțială sau integrală a datelor și a volumelor de lucru relevante de la furnizorul terț de servicii TIC relevant către un alt furnizor terț de servicii TIC, fie ca urmare a costurilor financiare semnificative, a timpului sau a altor resurse pe care le poate implica procesul de migrare, 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.

(3) În cazul în care furnizorul terț de servicii TIC face parte dintr-un grup, criteriile menționate la alineatul (2) sunt examinate în raport cu serviciile TIC furnizate de grup în ansamblul său.

(4) Furnizorii terți esențiali de servicii TIC care fac parte dintr-un grup desemnează o persoană juridică drept punct de coordonare pentru a asigura în mod adecvat reprezentarea și comunicarea cu supraveghetorul principal.

(5) Supraveghetorul principal notifică furnizorului terț de servicii TIC rezultatul evaluării care a dus la desemnarea menționată la alineatul (1) litera (a). În termen de șase săptămâni de la data notificării, furnizorul terț de servicii TIC îi poate transmite supraveghetorului principal o declarație motivată conținând orice informații relevante în scopul evaluării. Supraveghetorul principal analizează declarația motivată și poate solicita să îi fie furnizate informații suplimentare în termen de 30 de zile calendaristice de la primirea unei astfel de declarații.

După ce a desemnat un furnizor terț de servicii TIC ca fiind esențial, AES, prin intermediul Comitetului comun, informează furnizorul terț de servicii TIC cu privire la această desemnare și cu privire la data de la care va începe să facă efectiv obiectul activităților de supraveghere. Data respectivă trebuie să fie la cel mult o lună de la momentul notificării. Furnizorul terț de servicii TIC informează entitățile financiare cărora le furnizează servicii cu privire la desemnarea sa drept esențial.

(6) Comisia este împuternicită să adopte un act delegat în conformitate cu articolul 57 pentru a completa prezentul regulament prin precizarea mai în detaliu a criteriilor menționate la alineatul (2) de la prezentul articol, până la 17 iulie 2024.

(7) Nu se recurge la desemnarea menționată la alineatul (1) litera (a) decât după ce Comisia a adoptat un act delegat în conformitate cu alineatul (6).

(8) Desemnarea menționată la alineatul (1) litera (a) nu se aplică în ceea ce privește:

(i) entitățile financiare care furnizează servicii TIC altor entități financiare;

(ii) furnizorii 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;

(iii) furnizorii de servicii TIC intragrup;

(iv) furnizorii terți de servicii TIC care furnizează servicii TIC numai într-un stat membru unor entități financiare care își desfășoară activitatea numai în statul membru respectiv.

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

(10) În sensul alineatului (1) litera (a), autoritățile competente transmit, anual și agregat, Forumului de supraveghere instituit în temeiul articolului 32 rapoartele menționate la articolul 28 alineatul (3) al treilea paragraf. Forumul de supraveghere evaluează dependențele entităților financiare față de furnizorii terți de servicii TIC pe baza informațiilor primite de la autoritățile competente.

(11) Furnizorii terți de servicii TIC care nu sunt incluși în lista menționată la alineatul (9) pot solicita să fie desemnați ca fiind esențiali în conformitate cu alineatul (1) litera (a).

În scopul aplicării primului paragraf, furnizorul terț de servicii TIC transmite o cerere motivată către ABE, ESMA sau EIOPA care, prin intermediul Comitetului comun, decide dacă să desemneze respectivul furnizor terț de servicii TIC ca fiind esențial 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 șase luni de la primirea cererii.

(12) Entitățile financiare utilizează serviciile unui furnizor terț de servicii TIC stabilit într-o țară terță și care a fost desemnat ca fiind esențial în conformitate cu alineatul (1) litera (a) numai în cazul în care acesta din urmă a înființat o filială în Uniune în termen de 12 luni de la desemnare.

(13) Furnizorul terț esențial de servicii TIC menționat la alineatul (12) informează supraveghetorul principal cu privire la orice modificare a structurii conducerii filialei înființate în Uniune.

*Articolul 32*

**Structura cadrului de supraveghere**

(1) Comitetul comun, în conformitate cu articolul 57 alineatul (1) 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 31 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 de acte comune ale Comitetului comun în acest domeniu.

Forumul de supraveghere discută periodic despre 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 pentru furnizorii 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:

(a) președinții AES;

(b) un reprezentant la nivel înalt provenind din personalul actual al autorității competente relevante menționate la articolul 46 din fiecare stat membru;

(c) directorii executivi ai fiecărei AES și câte un reprezentant din partea Comisiei, CERS, BCE și ENISA, în calitate de observatori;

(d) după caz, un reprezentant suplimentar al unei autorități competente menționate la articolul 46 din fiecare stat membru, în calitate de observator;

(e) după caz, un reprezentant al autorităților competente desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555 responsabile de supravegherea unei entități esențiale sau importante căreia i se aplică directiva respectivă și care a fost desemnată drept furnizor terț esențial de servicii TIC, în calitate de observator.

Forumul de supraveghere poate, după caz, să solicite avizul unor experți independenți numiți în conformitate cu alineatul (6).

(5) Fiecare stat membru desemnează autoritatea competentă relevantă din cadrul personalului căreia este numit reprezentantul la nivel înalt menționat la alineatul (4) primul paragraf litera (b) și informează supraveghetorul principal în acest sens.

AES publică pe site-ul lor lista reprezentanților la nivel înalt, provenind din personalul actual al autorității competente relevante, desemnați de statele membre.

(6) Experții independenți menționați la alineatul (4) al doilea paragraf sunt numiți de Forumul de supraveghere dintr-un grup de rezervă de experți selectați în urma unui proces de candidatură public și transparent.

Experții independenți sunt numiți pe baza cunoștințelor și experienței lor în materie de stabilitate financiară, reziliență operațională digitală și securitate TIC. Aceștia acționează independent și obiectiv în interesul exclusiv al Uniunii în ansamblul său și nu solicită și nu primesc instrucțiuni din partea instituțiilor sau a organelor Uniunii, din partea vreunui guvern al unui stat membru sau din partea vreunui alt organism public sau privat.

(7) În conformitate cu articolul 16 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (UE) nr. 1095/2010, AES emit, până la 17 iulie 2024, în scopul aplicării prezentei secțiuni, orientări privind cooperarea dintre AES și autoritățile competente cuprinzând procedurile și condițiile detaliate pentru alocarea și executarea sarcinilor între autoritățile competente și AES, precum și detaliile privind schimburile de informații care sunt necesare pentru ca autoritățile competente să se asigure că recomandările adresate furnizorilor terți esențiali de servicii TIC în temeiul articolului 35 alineatul (1) litera (d) sunt urmate.

(8) Cerințele prevăzute în prezenta secțiune nu aduc atingere aplicării Directivei (UE) 2022/2555 și a altor norme ale Uniunii privind supravegherea aplicabilă furnizorilor de servicii de cloud computing.

(9) 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 33*

**Sarcinile supraveghetorului principal**

(1) Supraveghetorul principal, numit în conformitate cu articolul 31 alineatul (1) litera (b), efectuează supravegherea furnizorilor terți esențiali de servicii TIC atribuiți și este, cu privire la toate aspectele legate de supraveghere, punctul de contact principal pentru respectivii furnizori terți esențiali de servicii TIC.

(2) În scopul aplicării alineatului (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.

Evaluarea menționată la primul paragraf se axează în principal pe serviciile TIC furnizate de furnizorul terț esențial de servicii TIC care sprijină funcțiile critice sau importante ale entităților financiare. Atunci când este necesar pentru a aborda toate riscurile relevante, evaluarea respectivă se extinde la serviciile TIC care sprijină alte funcții decât cele critice sau importante.

(3) Evaluarea prevăzută la alineatul (2) cuprinde:

(a) cerințele 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 disponibilitate, autenticitate, integritate sau confidențialitate a datelor;

(b) securitatea fizică ce 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, politica de continuitate a activității TIC și planurile de răspuns și de recuperare în domeniul TIC;

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

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

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

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

(h) auditurile privind TIC;

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

(4) Pe baza evaluării prevăzute la alineatul (2) și în coordonare cu Rețeaua de supraveghere comună (RSC) menționată la articolul 34 alineatul (1), supraveghetorul principal adoptă un plan de supraveghere individual clar, detaliat și motivat care descrie obiectivele anuale de supraveghere și principalele acțiuni de supraveghere planificate pentru fiecare furnizor terț esențial de servicii TIC. Planul respectiv este comunicat în fiecare an furnizorului terț esențial de servicii TIC.

Înainte de adoptarea planului de supraveghere, supraveghetorul principal comunică proiectul planului de supraveghere furnizorului terț esențial de servicii TIC.

La primirea proiectului de plan de supraveghere, furnizorul terț esențial de servicii TIC poate prezenta, în termen de 15 zile calendaristice, o declarație motivată prin care să demonstreze impactul preconizat asupra clienților care sunt entități ce nu se încadrează în domeniul de aplicare al prezentului regulament și, după caz, să formuleze soluții pentru atenuarea riscurilor.

(5) Odată ce planurile de supraveghere anuale menționate la alineatul (4) au fost adoptate și notificate furnizorilor terți esențiali de servicii TIC, autoritățile competente pot lua măsuri privind acești furnizori terți esențiali de servicii TIC numai în acord cu supraveghetorul principal.

*Articolul 34*

**Coordonarea operațională a supraveghetorilor principali**

(1) Pentru a asigura o abordare coerentă a activităților de supraveghere și a permite coordonarea strategiilor generale de supraveghere și coeziunea abordărilor operaționale și a metodologiilor de lucru, cei trei supraveghetori principali numiți în conformitate cu articolul 31 alineatul (1) litera (b) instituie o RSC pentru a-și coordona acțiunile în cursul etapelor pregătitoare și al desfășurării activităților de supraveghere a furnizorilor terți esențiali de servicii TIC pe care îi supraveghează fiecare dintre ei, precum și în cursul oricărei acțiuni care ar putea fi necesară în temeiul articolului 42.

(2) În scopul aplicării alineatului (1), supraveghetorii principali elaborează un protocol de supraveghere comun în care precizează procedurile detaliate care trebuie urmate pentru realizarea coordonării curente și pentru asigurarea unor schimburi și reacții rapide. Protocolul este revizuit periodic pentru a reflecta nevoile operaționale, în special evoluția modalităților practice de supraveghere.

(3) Supraveghetorii principali pot solicita ad-hoc BCE și ENISA să ofere consiliere tehnică, să facă schimb de experiență practică sau să participe la anumite reuniuni de coordonare ale RSC.

*Articolul 35*

**Competențele supraveghetorului principal**

(1) În scopul îndeplinirii atribuțiilor care îi revin în temeiul prezentei secțiuni, supraveghetorul principal are următoarele competențe în ceea ce privește furnizorii terți esențiali de servicii TIC:

(a) de a solicita toate informațiile și documentele relevante în conformitate cu articolul 37;

(b) de a efectua investigații generale și inspecții în conformitate cu articolele 38 și, respectiv, 39;

(c) de a solicita, după încheierea activităților de supraveghere, rapoarte 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 emite recomandări privind domeniile menționate la articolul 33 alineatul (3), 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, potrivit cărora furnizorii terți esențiali de servicii TIC furnizează servicii TIC 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) orice subcontractare planificată, în cazul în care supraveghetorul principal consideră că subcontractarea în continuare, inclusiv acordurile de subcontractare pe care furnizorii terți esențiali de servicii TIC intenționează să le încheie cu furnizori terți de servicii TIC sau cu subcontractanți de servicii TIC stabiliți într-o țară terță, poate genera riscuri pentru furnizarea de servicii de către entitatea financiară sau riscuri pentru stabilitatea financiară, pe baza examinării informațiilor colectate în conformitate cu articolele 37 și 38;

(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 funcții critice sau importante ale entității financiare; și

— supraveghetorul principal consideră că utilizarea unei astfel de subcontractări prezintă un risc clar și grav pentru stabilitatea financiară a Uniunii sau pentru entitățile financiare, inclusiv pentru capacitatea entităților financiare de a se conforma cerințelor de supraveghere.

În scopul aplicării punctului (iv) de la prezenta literă, furnizorii terți de servicii TIC transmit informațiile privind subcontractarea supraveghetorului principal, utilizând modelul prevăzut la articolul 41 alineatul (1) litera (b).

(2) Atunci când exercită competențele prevăzute la prezentul articol, supraveghetorul principal:

(a) asigură o coordonare regulată în cadrul RSC și, în special, urmărește aplicarea unor abordări coerente, după caz, în ceea ce privește supravegherea furnizorilor terți esențiali de servicii TIC;

(b) ține seama în mod corespunzător de cadrul instituit prin Directiva (UE) 2022/2555 și, atunci când este necesar, consultă autoritățile competente relevante desemnate sau instituite în conformitate cu directiva respectivă, pentru a evita suprapunerea măsurilor tehnice și organizatorice care s-ar putea aplica furnizorilor terți esențiali de servicii TIC în temeiul directivei respective;

(c) urmărește să reducă la minimum, în măsura posibilului, riscul de perturbare a serviciilor furnizate de furnizori terți esențiali de servicii TIC unor clienți care sunt entități ce nu se încadrează în domeniul de aplicare al prezentului regulament.

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

Înainte de a emite recomandări în conformitate cu alineatul (1) litera (d), supraveghetorul principal îi oferă furnizorului terț de servicii TIC posibilitatea de a prezenta, în termen de 30 de zile calendaristice, informații relevante care să demonstreze impactul preconizat asupra clienților care sunt entități ce nu se încadrează în domeniul de aplicare al prezentului regulament și, după caz, să formuleze soluții pentru atenuarea riscurilor.

(4) Supraveghetorul principal informează RSC cu privire la rezultatul exercitării competențelor prevăzute la alineatul (1) literele (a) și (b). Supraveghetorul principal transmite fără întârzieri nejustificate rapoartele menționate la alineatul (1) litera (c) către RSC și către autoritățile competente ale entităților financiare care utilizează serviciile TIC ale respectivului furnizor terț esențial de servicii TIC.

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

(6) În cazul nerespectării totale sau parțiale a măsurilor care trebuie luate ca urmare a exercitării competențelor prevăzute la alineatul (1) literele (a), (b) și (c) și după expirarea unui termen de cel puțin 30 de zile calendaristice de la data la care furnizorul terț esențial de servicii TIC a fost notificat cu privire la măsurile respective, supraveghetorul principal adoptă o decizie prin care impune o penalitate cu titlu cominatoriu pentru a obliga furnizorul terț esențial de servicii TIC să se conformeze măsurilor respective.

(7) Penalitățile cu titlu cominatoriu prevăzute la alineatul (6) se impun pe zi de întârziere până când conformitatea este asigurată și pe o perioadă de maximum șase luni de la data notificării deciziei de impunere a unei penalități cu titlu cominatoriu furnizorului terț esențial de servicii TIC.

(8) Cuantumul penalității cu titlu cominatoriu, calculat de la data prevăzută în decizia de impunere a penalității cu titlu cominatoriu, este de până la 1 % din cifra de afaceri zilnică medie globală a furnizorului terț esențial de servicii TIC din exercițiul financiar precedent. La stabilirea cuantumului penalității cu titlu cominatoriu, supraveghetorul principal ține seama de următoarele criterii referitoare la nerespectarea măsurilor prevăzute la alineatul (6):

(a) gravitatea și durata neconformității;

(b) dacă neconformitatea a fost săvârșită în mod intenționat sau din neglijență;

(c) nivelul de cooperare al furnizorului terț de servicii TIC cu supraveghetorul principal.

În scopul aplicării primului paragraf, pentru a asigura o abordare coerentă, supraveghetorul principal efectuează consultări în cadrul RSC.

(9) Penalitățile cu titlu cominatoriu 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 este acordat accesul. Plângerile legate de neregulile survenite în cursul executării sunt de competența instanțelor judecătorești ale statului membru în cauză. Sumele aferente penalităților se alocă bugetului general al Uniunii Europene.

(10) Supraveghetorul principal 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.

(11) Înainte de a impune o penalitate cu titlu cominatoriu în temeiul alineatului (6), supraveghetorul principal oferă reprezentanților furnizorului terț esențial de servicii TIC care face obiectul procedurii 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 procedurii a avut ocazia să își prezinte observațiile.

Dreptul la apărare al persoanelor care fac obiectul procedurii se respectă pe deplin pe durata acesteia. Furnizorul terț esențial de servicii TIC care face obiectul procedurii are dreptul de a avea acces la dosar, sub rezerva interesului legitim al altor persoane de a-și proteja secretele comerciale. Dreptul de acces la dosar nu se extinde și la informațiile confidențiale sau la documentele interne de lucru ale supraveghetorului principal.

*Articolul 36*

**Exercitarea competențelor supraveghetorului principal în afara Uniunii**

(1) Atunci când obiectivele de supraveghere nu pot fi atinse prin intermediul interacțiunii cu filiala înființată potrivit dispozițiilor articolului 31 alineatul (12) sau prin exercitarea de activități de supraveghere la sedii situate în Uniune, supraveghetorul principal poate exercita competențele menționate la următoarele dispoziții, cu privire la orice sediu situat într-o țară terță care este deținut sau utilizat în orice mod în scopul furnizării de servicii către entități financiare din Uniune de către un furnizor terț esențial de servicii TIC, în legătură cu operațiunile, funcțiile sau serviciile sale comerciale, inclusiv orice birou, sediu, teren, clădire sau altă proprietate folosită cu scop administrativ, comercial sau operațional:

(a) la articolul 35 alineatul (1) litera (a); și

(b) la articolul 35 alineatul (1) litera (b), în conformitate cu articolul 38 alineatul (2) literele (a), (b) și (d) și articolul 39 alineatul (1) și alineatul (2) litera (a).

Competențele menționate la primul paragraf pot fi exercitate sub rezerva îndeplinirii tuturor condițiilor următoare:

(i) supraveghetorul principal consideră că efectuarea unei inspecții într-o țară terță este necesară pentru a-i permite să își îndeplinească pe deplin și în mod eficace sarcinile care îi revin în temeiul prezentului regulament;

(ii) inspecția într-o țară terță este direct legată de furnizarea de servicii TIC unor entități financiare din Uniune;

(iii) furnizorul terț esențial de servicii TIC în cauză este de acord cu efectuarea unei inspecții într-o țară terță; și

(iv) autoritatea relevantă din țara terță în cauză a fost notificată oficial de supraveghetorul principal și nu a formulat nicio obiecție cu privire la aceasta.

(2) Fără a aduce atingere competențelor instituțiilor Uniunii și, respectiv, ale statelor membre, în scopul aplicării alineatului (1), ABE, ESMA sau EIOPA încheie acorduri de cooperare administrativă cu autoritatea relevantă din țara terță pentru a permite buna desfășurare a inspecțiilor în țara terță în cauză de către supraveghetorul principal și echipa desemnată de acesta pentru misiunea sa în țara terță respectivă. Aceste acorduri de cooperare nu creează obligații juridice pentru Uniune și statele sale membre și nu împiedică statele membre și autoritățile lor competente să încheie acorduri bilaterale sau multilaterale cu țările terțe respective și cu autoritățile competente ale acestora.

Aceste acorduri de cooperare specifică cel puțin următoarele elemente:

(a) procedurile privind coordonarea activităților de supraveghere desfășurate în temeiul prezentului regulament și orice monitorizare analoagă a riscurilor TIC generate de părți terțe în sectorul financiar efectuată de autoritatea relevantă din țara terță în cauză, inclusiv detaliile privind transmiterea acordului acesteia din urmă pentru a permite efectuarea, de către supraveghetorul principal și echipa desemnată de acesta, a investigațiilor generale și a inspecțiilor la fața locului menționate la alineatul (1) primul paragraf pe teritoriul aflat sub jurisdicția sa;

(b) mecanismul de transmitere a oricăror informații relevante între ABE, ESMA sau EIOPA și autoritatea relevantă din țara terță în cauză, în special în legătură cu informațiile care pot fi solicitate de supraveghetorul principal în temeiul articolului 37;

(c) mecanismele prin care se realizează notificarea promptă de către autoritatea relevantă din țara terță în cauză a ABE, ESMA sau EIOPA cu privire la cazurile în care se consideră că un furnizor terț de servicii TIC stabilit într-o țară terță și desemnat ca fiind esențial în conformitate cu articolul 31 alineatul (1) litera (a) a încălcat cerințele pe care este obligat să le respecte în temeiul dreptului aplicabil al țării terțe în cauză atunci când furnizează servicii unor instituții financiare din țara terță respectivă, precum și măsurile corective și sancțiunile aplicate;

(d) transmiterea periodică de informații actualizate privind evoluțiile în materie de reglementare sau de supraveghere în ceea ce privește monitorizarea riscurilor TIC generate de părți terțe ale instituțiilor financiare din țara terță în cauză;

(e) detaliile pentru a permite, dacă este necesar, participarea unui reprezentant al autorității competente din țara terță la inspecțiile efectuate de supraveghetorul principal și de echipa desemnată.

(3) În cazul în care supraveghetorul principal nu este în măsură să desfășoare activitățile de supraveghere în afara Uniunii menționate la alineatele (1) și (2), supraveghetorul principal:

(a) își exercită competențele prevăzute la articolul 35 pe baza tuturor faptelor și documentelor de care dispune;

(b) documentează și explică orice consecință a imposibilității sale de a desfășura activitățile de supraveghere preconizate la care se referă prezentul articol.

Consecințele potențiale menționate la litera (b) de la prezentul alineat sunt luate în considerare în cadrul recomandărilor emise de supraveghetorul principal în temeiul articolului 35 alineatul (1) litera (d).

*Articolul 37*

**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 care îi revin 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 printr-o decizie 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 35 alineatul (6) în cazul în care informațiile solicitate sunt furnizate incomplet sau dacă aceste informații nu sunt furnizate în termenul menționat la litera (d) de la prezentul alineat;

(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 (denumită în continuare „Curtea de Justiție"), în conformitate cu articolele 60 și 61 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1094/2010 și (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 au în continuare întreaga responsabilitate în cazul în care informațiile furnizate sunt incomplete, incorecte sau induc în eroare.

(5) Supraveghetorul principal transmite fără întârziere o copie a deciziei prin care se solicită furnizarea de informații autorităților competente ale entităților financiare care folosesc serviciile furnizorilor terți esențiali de servicii TIC relevanți și RSC.

*Articolul 38*

**Investigații generale**

(1) Pentru a-și îndeplini sarcinile care îi revin în temeiul prezentului regulament, supraveghetorul principal, asistat de echipa de examinare comună menționată la articolul 40 alineatul (1), poate, atunci când este necesar, să efectueze investigații cu privire la furnizorii terți esențiali de servicii TIC.

(2) Supraveghetorul principal este abilitat:

(a) să analizeze 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 unor astfel de evidențe, date, documente care prevăd proceduri și ale oricăror alte materiale, precum și extrase din acestea;

(c) să convoace reprezentanții furnizorului terț esențial 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 pună întrebări oricărei alte persoane fizice sau juridice care acceptă să i se pună întrebări 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 celelalte 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 35 alineatul (6) aplicabile în cazul în care evidențele, datele, documentele care prevăd proceduri 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 esențiali 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 35 alineatul (6), 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 începerea investigației, supraveghetorul principal informează autoritățile competente ale entităților financiare care utilizează serviciile TIC ale respectivului furnizor terț esențial de servicii TIC cu privire la investigația preconizată și la identitatea persoanelor autorizate.

Supraveghetorul principal comunică RSC toate informațiile primite în temeiul primului paragraf.

*Articolul 39*

**Inspecții**

(1) Pentru a-și îndeplini sarcinile care îi revin în temeiul prezentului regulament, supraveghetorul principal, asistat de echipele de examinare comună menționate la articolul 40 alineatul (1), poate să aibă acces la orice sediu comercial, teren sau proprietate a furnizorilor terți de servicii TIC, cum ar fi sediile sociale, centrele de operațiuni sau sediile secundare, și poate să efectueze toate inspecțiile la fața locului necesare, precum și să efectueze inspecții la distanță.

În scopul exercitării competențelor menționate la primul paragraf, supraveghetorul principal consultă RSC.

(2) Funcționarii și celelalte persoane autorizate de supraveghetorul principal să efectueze o inspecție la fața locului sunt abilitați:

(a) să intre în orice astfel de sediu comercial, teren sau proprietate; și

(b) să sigileze orice astfel de sediu comercial**,** registre sau evidențe**,** pe perioada inspecției și în măsura în care acest lucru este necesar pentru inspecție.

Funcționarii și celelalte persoane autorizate de supraveghetorul principal 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 35 alineatul (6) în cazul în care reprezentanții furnizorilor terți esențiali de servicii TIC în cauză nu se supun inspecției.

(3) În timp util înainte de începerea inspecției, supraveghetorul principal 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 TIC către entități financiare.

(5) Înainte de orice inspecție la fața locului planificată, supraveghetorul principal le dă un preaviz rezonabil furnizorilor terți esențiali de servicii TIC, cu excepția cazului în care un astfel de preaviz nu este posibil din cauza unei situații de urgență sau de criză sau în cazul în care acesta 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 va începe inspecția și indică penalitățile cu titlu cominatoriu prevăzute la articolul 35 alineatul (6), 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 celelalte persoane autorizate de supraveghetorul principal constată că un furnizor terț esențial de servicii TIC se opune unei inspecții dispuse în temeiul prezentului articol, supraveghetorul principal informează furnizorul terț esențial de servicii TIC cu privire la consecințele unei astfel de opoziții, inclusiv cu privire la posibilitatea ca autoritățile competente ale entităților financiare relevante să solicite entităților financiare să înceteze acordurile contractuale încheiate cu respectivul furnizor terț esențial de servicii TIC.

*Articolul 40*

**Supravegherea permanentă**

(1) Atunci când desfășoară activități de supraveghere, în special investigații generale sau inspecții, supraveghetorul principal este asistat de o echipă de examinare comună, instituită pentru fiecare furnizor terț esențial de servicii TIC.

(2) Echipa de examinare comună menționată la alineatul (1) este formată din membri ai personalului:

(a) AES;

(b) autorităților competente relevante care supraveghează entitățile financiare cărora furnizorul terț esențial de servicii TIC le oferă servicii TIC;

(c) autorității naționale competente menționate la articolul 32 alineatul (4) litera (e), pe bază de voluntariat;

(d) unei autorități naționale competente din statul membru în care este stabilit furnizorul terț esențial de servicii TIC, pe bază de voluntariat.

Membrii echipei de examinare comună au cunoștințe de specialitate în domeniul TIC și în ceea ce privește riscurile operaționale. Echipa de examinare comună lucrează sub coordonarea unui membru desemnat al personalului supraveghetorului principal („coordonatorul supraveghetorului principal”).

(3) În termen de trei luni de la încheierea unei investigații sau a unei inspecții, supraveghetorul principal, după consultarea Forumului de supraveghere, adoptă recomandări care urmează a fi adresate furnizorului terț esențial de servicii TIC în temeiul competențelor menționate la articolul 35.

(4) Recomandările menționate la alineatul (3) se comunică imediat furnizorului terț esențial de servicii TIC și autorităților competente ale entităților financiare cărora acesta le furnizează servicii TIC.

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

*Articolul 41*

**Armonizarea condițiilor care permit desfășurarea activităților de supraveghere**

(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 de servicii TIC în cererea prin care solicită în mod voluntar să fie desemnați ca fiind esențiali în temeiul articolului 31 alineatul (11);

(b) conținutul, structura și formatul informațiilor care trebuie transmise, comunicate sau raportate de furnizorii terți de servicii TIC în temeiul articolului 35 alineatul (1), inclusiv modelul pentru furnizarea informațiilor privind acordurile de subcontractare;

(c) criteriile privind stabilirea componenței echipei de examinare comune, asigurând o participare echilibrată a membrilor personalului AES și a membrilor personalului autorităților competente relevante, precum și modul de desemnare, sarcinile și acordurile de lucru ale acestora;

(d) detaliile evaluării efectuate de autoritățile competente cu privire la măsurile luate de furnizorii terți esențiali de servicii TIC pe baza recomandărilor supraveghetorului principal în conformitate cu articolul 42 alineatul (3).

(2) AES transmit Comisiei aceste proiecte de standarde tehnice de reglementare până la 17 iulie 2024.

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

*Articolul 42*

**Acțiunile ulterioare întreprinse de autoritățile competente**

(1) În termen de 60 de zile calendaristice de la primirea recomandărilor emise de supraveghetorul principal în temeiul articolului 35 alineatul (1) litera (d), furnizorii terți esențiali de servicii TIC fie informează supraveghetorul principal cu privire la intenția lor de a urma recomandările, fie oferă o explicație cu privire la motivele pentru care nu vor urma recomandările respective. Supraveghetorul principal transmite imediat aceste informații autorităților competente ale entităților financiare în cauză.

(2) Supraveghetorul principal face publice cazurile în care un furnizor terț esențial de servicii TIC nu informează supraveghetorul principal în conformitate cu alineatul (1) sau cazurile în care explicația furnizată de furnizorul terț esențial de servicii TIC nu este considerată suficientă. Informațiile publicate dezvăluie identitatea furnizorului terț esențial de servicii TIC, precum și informații privind tipul și natura neconformității. Aceste informații se limitează la ceea ce este pertinent și proporțional în scopul asigurării informării publicului, cu excepția cazului în care această publicare ar cauza prejudicii disproporționate părților implicate sau ar putea periclita grav buna funcționare și integritatea piețelor financiare sau stabilitatea întregului sistem financiar al Uniunii sau a unei părți a acestuia.

Supraveghetorul principal informează furnizorul terț de servicii TIC cu privire la respectiva informare publică.

(3) Autoritățile competente informează entitățile financiare relevante cu privire la riscurile identificate în cadrul recomandărilor adresate furnizorilor terți esențiali de servicii TIC în conformitate cu articolul 35 alineatul (1) litera (d).

Atunci când gestionează riscuri TIC generate de părți terțe, entitățile financiare țin seama de riscurile menționate la primul paragraf.

(4) În cazul în care o autoritate competentă consideră că o entitate financiară, în cadrul activității sale de gestionare a riscurilor TIC generate de părți terțe, nu ține seama de riscurile specifice identificate în cadrul recomandărilor sau nu le contracarează suficient, aceasta notifică entitatea financiară cu privire la posibilitatea adoptării unei decizii, în termen de 60 de zile calendaristice de la primirea unei astfel de notificări, în temeiul alineatului (6), în lipsa unor acorduri contractuale adecvate care să aibă drept scop contracararea acestor riscuri.

(5) La primirea rapoartelor menționate la articolul 35 alineatul (1) litera (c) și înainte de a lua o decizie astfel cum se menționează la alineatul (6) de la prezentul articol, autoritățile competente pot, în mod voluntar, să consulte autoritățile competente desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555 responsabile de supravegherea unei entități esențiale sau importante căreia i se aplică directiva respectivă și care a fost desemnată drept furnizor terț esențial de servicii TIC.

(6) Autoritățile competente pot, ca măsură de ultimă instanță, în urma informării și, dacă este cazul, a consultării prevăzute la alineatele (4) și (5) din prezentul articol, în conformitate cu articolul 50, să adopte o decizie prin care să solicite entităților financiare să suspende temporar, parțial sau integral, utilizarea sau implementarea unui serviciu furnizat de furnizorul terț esențial de servicii TIC până la contracararea riscurilor identificate în cadrul recomandărilor 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.

(7) În cazul în care un furnizor terț esențial de servicii TIC refuză să accepte recomandările în baza unei abordări divergente față de cea recomandată de supraveghetorul principal, și o astfel de abordare divergentă ar putea avea un impact negativ asupra unui număr mare de entități financiare sau asupra unei părți semnificative a sectorului financiar, iar avertismentele individuale emise de autoritățile competente nu au avut drept rezultat abordări coerente care să atenueze riscul potențial la adresa stabilității financiare, supraveghetorul principal poate, după consultarea Forumului de supraveghere, să emită avize neobligatorii și fără caracter public adresate autorităților competente, pentru a promova măsuri ulterioare de supraveghere coerente și convergente, după caz.

(8) La primirea rapoartelor menționate la articolul 35 alineatul (1) litera (c), autoritățile competente, atunci când iau o decizie în conformitate cu alineatul (6) de la prezentul articol, țin seama de tipul și de amploarea riscului care nu a fost contracarat 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 prin neconformitate a fost facilitată sau ocazionată o infracțiune financiară sau dacă aceasta este imputabilă în alt mod neconformității;

(d) dacă neconformitatea a fost intenționată sau este rezultatul unei neglijențe;

(e) dacă suspendarea sau încetarea acordurilor contractuale dă naștere unui risc la adresa continuității activităților economice ale entității financiare în pofida eforturilor acesteia de a evita perturbarea furnizării serviciilor sale;

(f) după caz, avizul autorităților competente desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555 responsabile de supravegherea unei entități esențiale sau importante căreia i se aplică directiva respectivă și care a fost desemnată drept furnizor terț esențial de servicii TIC, aviz solicitat în mod voluntar în conformitate cu alineatul (5) de la prezentul articol.

Autoritățile competente le acordă entităților financiare perioada de timp necesară pentru a le permite să adapteze acordurile contractuale cu furnizorii terți esențiali de servicii TIC pentru a evita apariția unor efecte negative asupra rezilienței lor operaționale digitale și pentru a le permite să implementeze strategiile de ieșire și planurile de tranziție, astfel cum sunt menționate la articolul 28.

(9) Decizia menționată la alineatul (6) de la prezentul articol se notifică membrilor Forumului de supraveghere menționat la articolul 32 alineatul (4) literele (a), (b) și (c) și RSC.

Furnizorii terți esențiali de servicii TIC vizați de deciziile prevăzute la alineatul (6) cooperează pe deplin cu entitățile financiare afectate, în special în contextul procesului de suspendare sau de încetare a acordurilor lor contractuale.

(10) Autoritățile competente informează periodic supraveghetorul principal cu privire la abordările urmate și măsurile luate în cadrul atribuțiilor lor de supraveghere în ceea ce privește entitățile financiare, precum și cu privire la acordurile contractuale încheiate de entitățile financiare în cazul în care furnizorii terți esențiali de servicii TIC nu au acceptat, parțial sau în întregime, recomandările adresate de supraveghetorul principal.

(11) Supraveghetorul principal poate, la cerere, să furnizeze clarificări suplimentare cu privire la recomandările emise pentru a îndruma autoritățile competente cu privire la măsurile ulterioare.

*Articolul 43*

**Taxele de supraveghere**

(1) În conformitate cu actul delegat menționat la alineatul (2) de la prezentul articol, supraveghetorul principal percepe de la furnizorii terți esențiali de servicii TIC taxe care acoperă integral cheltuielile necesare ale supraveghetorului principal 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 echipa de examinare comună prevăzută la articolul 40, precum și a costurilor aferente consultanței furnizate de experții independenți menționați la articolul 32 alineatul (4) al doilea paragraf, în legătură cu aspecte care intră în sfera activităților de supraveghere directă.

Cuantumul unei taxe percepute de la un furnizor terț esențial de servicii TIC acoperă toate costurile care decurg din efectuarea sarcinilor stabilite în prezenta secțiune și este proporțional cu cifra sa de afaceri.

(2) Comisia este împuternicită să adopte un act delegat în conformitate cu articolul 57 pentru a completa prezentul regulament prin stabilirea cuantumului taxelor și a modalității de plată a acestora, până la 17 iulie 2024.

*Articolul 44*

**Cooperarea internațională**

(1) Fără a aduce atingere articolului 36, ABE, ESMA și EIOPA pot, în conformitate cu articolul 33 din Regulamentele (UE) nr. 1093/2010, (UE) nr. 1095/2010 și, respectiv, (UE) nr. 1094/2010, 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 și funcționarea pieței interne.

***CAPITOLUL VI***

***Acorduri privind schimbul de informații***

*Articolul 45*

**Acorduri privind schimbul de informații referitoare la 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 creșterea gradului de conștientizarea cu privire la amenințările cibernetice, limitarea sau împiedicarea capacității de propagare a amenințărilor cibernetice, sprijinirea capacităților de apărare, 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 privind schimbul de informații care protejează natura potențial sensibilă a informațiilor partajate și care sunt reglementate de norme de conduită care respectă pe deplin secretul comercial, protecția datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 și orientările privind politica în domeniul concurenței.

(2) În scopul aplicării alineatului (1) litera (c), acordurile privind schimbul de informații definesc condițiile de participare și, după caz, stabilesc detaliile privind implicarea autorităților publice și calitatea în care acestea pot fi asociate la acordurile privind schimbul de informații, implicarea furnizorilor terți de servicii TIC și elementele operaționale, inclusiv utilizarea platformelor informatice specifice.

(3) Entitățile financiare informează autoritățile competente cu privire la participarea lor la acordurile privind schimbul de informații menționate la alineatul (1), în momentul validării sau, după caz, al încetării participării lor, odată ce aceasta începe să producă efecte.

*CAPITOLUL VII*

***Autoritățile competente***

*Articolul 46*

**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, respectarea prezentului regulament este asigurată de următoarele autorități competente în conformitate cu prerogativele conferite prin actele juridice respective:

(a) pentru instituțiile de credit și pentru instituțiile exceptate în temeiul Directivei 2013/36/UE, autoritatea competentă desemnată în conformitate cu articolul 4 din directiva respectivă, iar pentru instituțiile de credit clasificate ca fiind semnificative în conformitate cu articolul 6 alineatul (4) din Regulamentul (UE) nr. 1024/2013, BCE, în conformitate cu competențele și atribuțiile conferite prin regulamentul respectiv;

(b) pentru instituțiile de plată, inclusiv instituțiile de plată exceptate în temeiul Directivei (UE) 2015/2366, instituțiile emitente de monedă electronică, inclusiv cele exceptate în temeiul Directivei 2009/110/CE, și prestatorii de servicii de informare cu privire la conturi menționați la articolul 33 alineatul (1) din Directiva (UE) 2015/2366, autoritatea competentă desemnată în conformitate cu articolul 22 din Directiva (UE) 2015/2366;

(c) pentru firmele de investiții, autoritatea competentă desemnată în conformitate cu articolul 4 din Directiva (UE) 2019/2034 a Parlamentului European și a Consiliului ([38]);

(d) pentru furnizorii de servicii de criptoactive autorizați în temeiul Regulamentului privind piețele criptoactivelor și pentru emitenții de tokenuri raportate la active, autoritatea competentă desemnată în conformitate cu dispozițiile relevante din regulamentul respectiv;

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

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

(g) 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 și autoritatea competentă definită la articolul 2 alineatul (1) punctul 18 din Regulamentul (UE) nr. 600/2014;

(h) pentru registrele centrale de tranzacții, autoritatea competentă desemnată în conformitate cu articolul 22 din Regulamentul (UE) nr. 648/2012;

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

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

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

(l) 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;

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

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

(o) pentru administratorii de indici de referință critici, autoritatea competentă desemnată în conformitate cu articolele 40 și 41 din Regulamentul (UE) 2016/1011;

([38]) Directiva (UE) 2019/2034 a Parlamentului European și a Consiliului din 27 noiembrie 2019 privind supravegherea prudențială a firmelor de investiții și de modificare a Directivelor 2002/87/CE, 2009/65/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE și 2014/65/UE (JO L 314, 5.12.2019, p. 64).

(p) pentru furnizorii de servicii de finanțare participativă, autoritatea competentă desemnată în conformitate cu articolul 29 din Regulamentul (UE) 2020/1503;

(q) 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 47*

**Cooperarea cu structurile și autoritățile înființate prin Directiva (UE) 2022/2555**

(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 14 din Directiva (UE) 2022/2555, AES și autoritățile competente pot participa la activitățile Grupului de cooperare în ceea ce privește chestiuni care privesc activitățile lor de supraveghere în legătură cu entitățile financiare. AES și autoritățile competente pot solicita să fie invitate să participe la activitățile Grupului de cooperare cu privire la chestiuni legate de entitățile esențiale sau importante cărora li se aplică Directiva (UE) 2022/2555 și care au fost, de asemenea, desemnate drept furnizori terți esențiali de servicii TIC în temeiul articolului 31 din prezentul regulament.

(2) După caz, autoritățile competente se pot consulta și pot face schimb de informații cu punctele unice de contact și cu echipele CSIRT desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555.

(3) După caz, autoritățile competente pot solicita orice tip de consultanță și asistență tehnică relevantă din partea autorităților competente desemnate sau stabilite în conformitate cu Directiva (UE) 2022/2555 și pot stabili acorduri de cooperare pentru a permite crearea unor mecanisme de coordonare eficace și rapide.

(4) Acordurile menționate la alineatul (3) de la prezentul articol pot specifica, printre altele, procedurile pentru coordonarea activităților de supraveghere și, respectiv, de control în ceea ce privește entitățile esențiale sau importante cărora li se aplică Directiva (UE) 2022/2555 și care au fost desemnate drept furnizori terți esențiali de servicii TIC în temeiul articolului 31 din prezentul regulament, inclusiv pentru efectuarea, în conformitate cu dreptul intern, a investigațiilor și a inspecțiilor la fața locului, precum și pentru mecanismele privind schimbul de informații dintre autoritățile competente în temeiul prezentului regulament și autoritățile competente desemnate sau stabilite în conformitate cu directiva respectivă, care include accesul la informațiile solicitate de autoritățile din urmă.

*Articolul 48*

**Cooperarea între autorități**

(1) Autoritățile competente cooperează îndeaproape între ele și, după caz, cu supraveghetorul principal.

(2) Autoritățile competente și supraveghetorul principal își transmit reciproc, în timp util, toate informațiile relevante privind furnizorii terți esențiali de servicii TIC care sunt necesare pentru îndeplinirea sarcinilor care le revin în temeiul prezentului regulament, în special în legătură cu riscurile identificate, cu abordările și cu măsurile adoptate în cadrul sarcinilor de supraveghere ale supraveghetorului principal.

*Articolul 49*

**Exerciții, comunicare și cooperare transsectoriale în domeniul financiar**

(1) AES, prin intermediul Comitetului comun și în colaborare cu autoritățile competente, cu autoritățile de rezoluție menționate la articolul 3 din Directiva 2014/59/UE, cu BCE, cu Comitetul unic de rezoluție în ceea ce privește informațiile referitoare la entitățile care intră sub incidența Regulamentului (UE) nr. 806/2014**,** cu CERS și cu ENISA, după caz, pot stabili mecanisme care să permită schimbul de practici eficace între sectoarele financiare în vederea îmbunătățirii gradului de conștientizare a 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.

Exercițiile respective pot, după caz, să testeze și dependențele sectorului financiar de alte sectoare economice.

(2) Autoritățile competente, AES și BCE cooperează strâns și fac schimb de informații pentru a-și îndeplini atribuțiile prevăzute la articolele 47-54. 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 50*

**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 competentă le consideră relevante pentru îndeplinirea sarcinilor sale și competența de a primi sau de a face o copie a acestora;

(b) competența de a efectua inspecții la fața locului sau investigații, incluzând, printre altele, următoarele activități:

(i) convocarea reprezentanților entităților financiare pentru explicații verbale sau scrise cu privire la fapte sau documente referitoare la obiectul și scopul investigației și înregistrarea răspunsurilor;

(ii) punerea de întrebări oricărei alte persoane fizice sau juridice care acceptă să i se pună întrebări în scopul colectării de informații referitoare la obiectul unei 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 52, 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 și 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 unei dispoziții prin care i se cere persoanei fizice sau juridice să înceteze comportamentul care încalcă prezentul regulament și să se abțină de la repetarea comportamentului respectiv;

(b) solicitarea încetării temporare sau permanente a oricărei practici sau a 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 alineatul (2) litera (c) și alineatul (4) se aplică unor persoane juridice, statele membre conferă autorităților competente competența de a aplica sancțiunile administrative și măsurile de remediere, 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 51*

**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 50 în conformitate cu cadrele lor juridice naționale, dacă este cazul, după cum urmează:

(a) în mod direct;

(b) în colaborare cu alte autorități;

(c) sub responsabilitate proprie prin delegare către alte autorități; sau

(d) prin sesizarea autorităților judiciare competente.

(2) La stabilirea tipului și a nivelului unei sancțiuni administrative sau al unei măsuri de remediere care urmează să fie impuse în temeiul articolului 50, autoritățile competente iau în considerare măsura în care încălcarea este intenționată sau rezultă din neglijență și toate celelalte circumstanțe relevante, inclusiv, după caz, următoarele elemente:

(a) importanța semnificativă, gravitatea și durata încălcării;

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

(c) soliditatea 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 terți 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 fizică sau juridică respectivă;

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

*Articolul 52*

**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 autoritățile judiciare penale 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 aplicării prezentului regulament.

*Articolul 53*

**Obligații de notificare**

Statele membre notifică actele cu putere de lege și actele administrative de punere în aplicare a prezentului capitol, inclusiv orice dispoziții relevante de drept penal, Comisiei, ESMA, ABE și EIOPA până la 17 ianuarie 2025. Statele membre înștiințează fără întârzieri nejustificate Comisia, ESMA, ABE și EIOPA cu privire la orice modificare ulterioară a acestor acte.

*Articolul 54*

**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 face obiectul niciunei căi de atac 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, comportând riscuri cu privire la protecția datelor cu caracter personal, 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, prejudicii 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 când toate motivele pentru nepublicare încetează;

(b) publică decizia menținând anonimatul persoanei în cauză, în conformitate cu dreptul intern; 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 clemența sancțiunii impuse.

(4) În cazul unei decizii de a publica sancțiunea administrativă menținând anonimatul persoanei în cauză 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 numai pe perioada care este necesară pentru ca prezentul articol să își producă efectele. Această perioadă nu poate depăși cinci ani de la data publicării.

*Articolul 55*

**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 respectivele autorități competente i-au delegat competențele lor, inclusiv auditorilor și experților contractați de acestea.

(3) Informațiile care fac obiectul secretului profesional, inclusiv schimbul de informații între autoritățile competente în temeiul prezentului regulament și autoritățile competente desemnate sau instituite în conformitate cu Directiva (UE) 2022/2555, nu se comunică niciunei alte persoane sau autorități, cu excepția cazului în care acest lucru este prevăzut de dreptul Uniunii sau de dreptul intern.

(4) Toate informațiile care fac obiectul unor schimburi între autoritățile competente în temeiul prezentului regulament și care privesc condițiile comerciale sau operaționale și alte chestiuni economice sau personale sunt considerate confidențiale și intră sub incidența obligației referitoare la secretul 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 desfășurarea unei proceduri judiciare.

*Articolul 56*

**Protecția datelor**

(1) AES și autoritățile competente sunt autorizate să prelucreze date cu caracter personal numai în cazul în care acest lucru este necesar în scopul îndeplinirii obligațiilor și sarcinilor care le revin în temeiul prezentului regulament, în special în ceea ce privește investigarea, realizarea de inspecții, solicitarea de informații, comunicarea, publicarea, evaluarea, verificarea, evaluarea și elaborarea de planuri de supraveghere. Datele cu caracter personal se prelucrează în conformitate cu Regulamentul (UE) 2016/679 sau cu Regulamentul (UE) 2018/1725, în funcție de care dintre acestea este aplicabil.

(2) Cu excepția cazului în care se prevede altfel în alte acte sectoriale, datele cu caracter personal menționate la alineatul (1) se păstrează până la îndeplinirea atribuțiilor de supraveghere aplicabile și, în orice caz, pentru o perioadă maximă de 15 ani, cu excepția cazului în care o procedură judiciară în curs necesită păstrarea acestor date pentru o perioadă mai lungă.

*CAPITOLUL VIII*

***Acte delegate***

*Articolul 57*

**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 31 alineatul (6) și la articolul 43 alineatul (2) se conferă Comisiei pe o perioadă de cinci ani de la 17 ianuarie 2024. Comisia elaborează un raport privind delegarea de competențe cu cel puțin nouă luni înainte de încheierea perioadei de cinci ani. Delegarea de competențe se prelungește tacit cu perioade de timp identice, cu excepția cazului în care Parlamentul European sau Consiliul se opune prelungirii respective cu cel puțin trei luni înainte de încheierea fiecărei perioade.

(3) Delegarea de competențe menționată la articolul 31 alineatul (6) și la articolul 43 alineatul (2) poate fi revocată oricând 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) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

(6) Un act delegat adoptat în temeiul articolului 31 alineatul (6) și al articolului 43 alineatul (2) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de trei luni de la notificarea acestuia către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu trei luni la inițiativa Parlamentului European sau a Consiliului.

*CAPITOLUL IX*

***Dispoziții tranzitorii și finale***

Secțiunea I

*Articolul 58*

**Clauza de reexaminare**

(1) Până la 17 ianuarie 2028, după ce se consultă cu AES și CERS, după caz, Comisia efectuează o reexaminare și prezintă un raport Parlamentului European și Consiliului, însoțit, dacă este cazul, de o propunere legislativă. Reexaminarea include cel puțin următoarele aspecte:

(a) criteriile pentru desemnarea furnizorilor terți esențiali de servicii TIC în conformitate cu articolul 31 alineatul (2);

(b) caracterul voluntar al notificării amenințărilor cibernetice semnificative menționat la articolul 19;

(c) regimul menționat la articolul 31 alineatul (12) și competențele supraveghetorului principal prevăzute la articolul 35 alineatul (1) litera (d) punctul (iv) prima liniuță, în vederea evaluării eficacității dispozițiilor respective în ceea ce privește asigurarea unei supravegheri eficace a furnizorilor terți esențiali de servicii TIC stabiliți într-o țară terță și necesitatea de a înființa o filială în Uniune.

În scopul aplicării primului paragraf de la prezenta literă, reexaminarea include o analiză a regimului menționat la articolul 31 alineatul (12), inclusiv a condițiilor de acces al entităților financiare din Uniune la servicii din țări terțe și a disponibilității unor astfel de servicii pe piața Uniunii, și ține seama de evoluția piețelor serviciilor care fac obiectul prezentului regulament, de experiența practică a entităților financiare și a supraveghetorilor financiari în ceea ce privește aplicarea și, respectiv, supravegherea regimului respectiv, precum și de orice evoluții relevante în materie de reglementare și de supraveghere care au loc la nivel internațional;

(d) oportunitatea includerii în domeniul de aplicare al prezentului regulament a entităților financiare menționate la articolul 2 alineatul (3) litera (e) care recurg la sisteme de vânzări automatizate, ținând seama de evoluțiile viitoare ale pieței în ceea ce privește utilizarea unor astfel de sisteme;

(e) funcționarea și eficacitatea RSC în ceea ce privește sprijinirea coerenței supravegherii și a eficienței schimbului de informații în interiorul cadrului de supraveghere.

(2) În contextul reexaminării Directivei (UE) 2015/2366, Comisia evaluează necesitatea unei mai mari reziliențe cibernetice a sistemelor de plăți și a activităților de prelucrare a plăților, precum și oportunitatea extinderii domeniului de aplicare al prezentului regulament la operatorii sistemelor de plată și la entitățile implicate în activitățile de prelucrare a plăților. În lumina acestei evaluări, Comisia prezintă Parlamentului European și Consiliului, în cadrul reexaminării Directivei (UE) 2015/2366, un raport până cel târziu la 17 iulie 2023.

Pe baza respectivului raport de reexaminare și după consultarea AES, BCE și CERS, Comisia poate prezenta, dacă este cazul și ca parte a propunerii legislative pe care o poate adopta în temeiul articolului 108 al doilea paragraf din Directiva (UE) 2015/2366, o propunere urmărind să asigure faptul că toți operatorii sistemelor de plată și entitățile implicate în activitățile de prelucrare a plăților fac obiectul unei supravegheri adecvate, ținând seama în același timp de supravegherea existentă din partea băncilor centrale.

(3) Până la 17 ianuarie 2026, după consultarea AES și a Comitetului Organismelor Europene de Supraveghere a Auditului, Comisia efectuează o reexaminare și prezintă Parlamentului European și Consiliului un raport, însoțit, după caz, de o propunere legislativă, cu privire la oportunitatea unor cerințe mai stricte pentru auditorii statutari și firmele de audit în ceea ce privește reziliența operațională digitală, prin includerea auditorilor statutari și a firmelor de audit în domeniul de aplicare al prezentului regulament sau prin intermediul unor modificări ale Directivei 2006/43/CE a Parlamentului European și a Consiliului ([39]).

Secțiunea II

## Modificări

*Articolul 59*

### Modificarea Regulamentului (CE) nr. 1060/2009

Regulamentul (CE) nr. 1060/2009 se modifică după cum urmează:

1. În anexa I 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) 2022/2554 al Parlamentului European și al Consiliului (*).

(*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).”

2. În anexa III, punctul 12 se înlocuiește cu următorul text:

„12. Agenția de rating de credit încalcă articolul 6 alineatul (2), coroborat cu punctul 4 din anexa I secțiunea A, prin faptul că nu dispune de proceduri contabile sau administrative sigure, de mecanisme de control intern, de proceduri eficiente de evaluare a riscurilor sau de dispozitive eficiente de control și de salvgardare pentru gestionarea sistemelor TIC în conformitate cu Regulamentul (UE) 2022/2554 sau prin faptul că nu pune în aplicare sau nu menține proceduri decizionale ori structuri organizaționale în conformitate cu punctul respectiv.”

*Articolul 60*

### Modificarea 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) 2022/2554 al Parlamentului European și al Consiliului (*).

(*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).”;

([39]) Directiva 2006/43/CE a Parlamentului European și a Consiliului din 17 mai 2006 privind auditul legal al conturilor anuale și al conturilor consolidate, de modificare a Directivelor 78/660/CEE și 83/349/CEE ale Consiliului și de abrogare a Directivei 84/253/CEE a Consiliului (JO L 157, 9.6.2006, p. 87).

(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 adecvat de recuperare în caz de dezastru, care includ o politică de continuitate a activității TIC și planuri de răspuns și de recuperare în domeniul TIC instituite și puse în aplicare în conformitate cu Regulamentul (UE) 2022/2554, 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:

„(3) 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 politica de continuitate a activității TIC și planurile de recuperare în caz de dezastru în domeniul TIC."

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 și prin dezvoltarea unor sisteme, mijloace de control și proceduri adecvate, inclusiv sisteme TIC gestionate în conformitate cu Regulamentul (UE) 2022/2554.

(2) Registrele centrale de tranzacții prevăd, aplică și mențin o politică adecvată de continuitate a activității și un plan adecvat de recuperare în caz de dezastru, care includ o politică de continuitate a activității TIC și planuri de răspuns și de recuperare în domeniul TIC instituite în conformitate cu Regulamentul (UE) 2022/2554, cu scopul de a asigura menținerea funcțiilor lor, reluarea rapidă a operațiunilor și îndeplinirea obligațiilor."

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

6. În anexa I, secțiunea II se modifică după cum urmează:

(a) literele (a) și (b) se înlocuiesc cu următorul text:

„(a) un registru central de tranzacții încalcă articolul 79 alineatul (1) dacă nu identifică sursele de risc operațional și nu reduce la minimum riscurile respective prin dezvoltarea unor sisteme, mijloace de control și proceduri adecvate, inclusiv sisteme TIC gestionate în conformitate cu Regulamentul (UE) 2022/2554;

(b) un registru central de tranzacții încalcă articolul 79 alineatul (2) dacă nu prevede, nu aplică sau nu menține o politică adecvată de continuitate a activității și un plan adecvat de redresare în caz de dezastru instituite în conformitate cu Regulamentul (UE) 2022/2554, cu scopul de a asigura menținerea funcțiilor sale, reluarea rapidă a operațiunilor și îndeplinirea obligațiilor;";

(b) litera (c) se elimină.

7. Anexa III se modifică după cum urmează:

(a) secțiunea II se modifică după cum urmează:

(i) litera (c) se înlocuiește cu următorul text:

„(c) CPC de nivel 2 încalcă articolul 26 alineatul (3) dacă nu mențin sau nu utilizează o structură organizatorică care să asigure continuitatea și funcționarea corespunzătoare în cursul prestării serviciilor și al desfășurării activităților lor sau dacă nu utilizează sisteme, resurse sau proceduri adecvate și proporționale, inclusiv sisteme TIC gestionate în conformitate cu Regulamentul (UE) 2022/2554";

(ii) litera (f) se elimină;

(b) în secțiunea III, litera (a) se înlocuiește cu următorul text:

„(a) CPC de nivel 2 încalcă articolul 34 alineatul (1) dacă nu prevăd, aplică sau mențin o politică adecvată de continuitate a activității și un plan adecvat de răspuns și de recuperare instituite în conformitate cu Regulamentul (UE) 2022/2554, cu scopul de a asigura conservarea funcțiilor lor, reluarea rapidă a operațiunilor și îndeplinirea obligațiilor CPC, care să permită cel puțin reluarea tuturor tranzacțiilor aflate în curs în momentul întreruperii, astfel încât CPC să poată continua să funcționeze în condiții de certitudine și să efectueze decontarea la data stabilită;”.

*Articolul 61*

**Modificarea 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) 2022/2554 al Parlamentului European și al Consiliului (*), precum și prin orice alte instrumente, mecanisme de control și proceduri adecvate relevante pentru alte tipuri de riscuri operaționale, inclusiv pentru toate sistemele de decontare a titlurilor de valoare pe care le exploatează.

_____

(*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).”

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 o politică adecvată de continuitate a activității și un plan adecvat de recuperare în caz de dezastru, care includ o politică de continuitate a activității TIC și planuri de răspuns și de recuperare în domeniul TIC instituite în conformitate cu Regulamentul (UE) 2022/2554, 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 12 alineatele (5) și (7) din Regulamentul (UE) 2022/2554.”

4. Alineatul (6) se înlocuiește cu următorul text:

„(6) 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:

„(7) 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 continuitate a activității și planurile de recuperare în caz de dezastru menționate la alineatele (3) și (4), precum și modalitățile de evaluare a acestora.”

*Articolul 62*

**Modificarea 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 înlocuiește cu următorul text:

   „(4) APA respectă cerințele privind securitatea rețelelor și a sistemelor informatice prevăzute în Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului (*).

   _____

   (*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).";

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

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

2. Articolul 27h se modifică după cum urmează:

   (a) alineatul (5) se înlocuiește cu următorul text:

   „(5) CTP respectă cerințele privind securitatea rețelelor și a sistemelor informatice prevăzute în Regulamentul (UE) 2022/2554.";

   (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 înlocuiește cu următorul text:

   „(3) ARM respectă cerințele privind securitatea rețelelor și a sistemelor informatice prevăzute în Regulamentul (UE) 2022/2554.";

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

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

*Articolul 63*

**Modificarea Regulamentului (UE) 2016/1011**

La articolul 6 din Regulamentul (UE) 2016/1011 se adaugă următorul alineat:

„(6) Pentru indicii de referință critici, administratorul dispune de proceduri administrative și contabile sigure, de mecanisme de control intern, de proceduri eficace de evaluare a riscurilor și de mecanisme eficiente de control și de salvgardare pentru gestionarea sistemelor TIC în conformitate cu Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului (*).

_____

(*) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1)."

*Articolul 64*

**Intrarea în vigoare și aplicarea**

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

Se aplică de la 17 ianuarie 2025.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Strasbourg, 14 decembrie 2022.

| *Pentru Parlamentul European* | *Pentru Consiliu* |
|---|---|
| *Președinta* | *Președintele* |
| R. METSOLA | M. BEK |