III

(Acte pregătitoare)

BANCA CENTRALĂ EUROPEANĂ

AVIZUL BĂNCII CENTRALE EUROPENE

din 4 iunie 2021

cu privire la o propunere de regulament al Parlamentului European și al Consiliului privind reziliența operațională digitală a sectorului financiar

(CON/2021/20)

(2021/C 343/01)

Introducere și temei juridic

La 22, 23 și 29 decembrie 2020, Banca Centrală Europeană (BCE) a primit din partea Consiliului Uniunii Europene și, respectiv, a Parlamentului European solicitări de emitere a unui aviz cu privire la o propunere de regulament al Parlamentului European și a Consiliului privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014 și (UE) nr. 909/2014 ([1]) (denumit în continuare „regulamentul propus") și o propunere de directivă de modificare a Directivelor 2006/43/CE, 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 și (UE) 2016/2341 ([2]) (denumită în continuare „directiva de modificare propusă", împreună cu regulamentul propus, denumite în mod colectiv „actele propuse").

Competența BCE de a emite un aviz se bazează pe articolul 127 alineatul (4) și pe articolul 282 alineatul (5) din Tratatul privind funcționarea Uniunii Europene, întrucât actele propuse conțin dispoziții care intră în sfera de competență a BCE, în special definirea și punerea în aplicare a politicii monetare, promovarea bunei funcționări a sistemelor de plăți, contribuția la buna desfășurare a politicilor promovate de autoritățile competente în ceea ce privește stabilitatea sistemului financiar și atribuțiile BCE privind supravegherea prudențială a instituțiilor de credit în temeiul articolului 127 alineatul (2) prima și a patra liniuță, al articolului 127 alineatul (5) și al articolului 127 alineatul (6) din tratat. În conformitate cu articolul 17.5 prima teză din Regulamentul de procedură al Băncii Centrale Europene, Consiliul guvernatorilor adoptă prezentul aviz.

1. Observații generale

1.1 BCE consideră binevenită propunerea de regulament, care vizează consolidarea securității cibernetice și a rezilienței operaționale a sectorului financiar. În special, BCE apreciază obiectivul regulamentului propus de a elimina obstacolele din calea instituirii și funcționării pieței interne de servicii financiare și de a îmbunătăți instituirea și funcționarea acesteia prin armonizarea normelor aplicabile în domeniul gestionării riscurilor privind tehnologia informației și a comunicațiilor (TIC), al raportării și testării cu privire la acestea și al riscurilor privind TIC generate de părți terțe. În plus, BCE apreciază obiectivul regulamentului propus de a raționaliza și de a armoniza orice suprapunere a cerințelor de reglementare sau a așteptărilor în materie de supraveghere care se aplică în prezent entităților financiare în temeiul dreptului Uniunii.

1.2 BCE înțelege că regulamentul propus reprezintă, în ceea ce privește entitățile financiare identificate ca operatori de servicii esențiale ([3]), legislație sectorială specifică (lex specialis) în conformitate cu sensul stabilit la articolul 1 alineatul (7) din Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului ([4]) (denumită în continuare „Directiva NIS"); aceasta implică faptul că cerințele din regulamentul propus ar prevala, în principiu, asupra Directivei NIS. În practică, entitățile financiare identificate ca operatori de servicii esențiale ([5]) ar raporta, printre altele, incidentele în conformitate cu regulamentul propus, iar nu cu Directiva

([1]) COM(2020) 595 final.
([2]) COM(2020) 596 final.
([3]) A se vedea articolul 1 alineatul (2) din regulamentul propus.
([4]) Directive (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).
([5]) A se vedea articolul 5 din Directiva NIS.

NIS. Deși BCE consideră binevenită reducerea cerințelor care s-ar putea suprapune pentru entitățile financiare în domeniul raportării incidentelor, ar trebui să se acorde mai multă atenție interacțiunii dintre propunerea de regulament și Directiva NIS. De exemplu, în temeiul regulamentului propus, un furnizor terț de servicii TIC ([6]) ar putea face obiectul unor recomandări emise de supervizorul principal ([7]). În același timp, același furnizor terț de servicii TIC poate fi clasificat ca operator de servicii esențiale în temeiul Directivei NIS și poate face obiectul unor instrucțiuni obligatorii emise de autoritatea competentă ([8]). În acest caz, furnizorul terț de servicii TIC ar putea face obiectul unor recomandări contradictorii emise în temeiul regulamentului propus și al instrucțiunilor obligatorii emise în temeiul Directivei NIS. BCE sugerează ca organele legislative ale Uniunii să reflecteze în continuare asupra eventualelor neconcordanțe dintre regulamentul propus și Directiva NIS, care ar putea împiedica armonizarea și reducerea cerințelor care se suprapun și sunt contradictorii pentru entitățile financiare.

1.3 BCE înțelege, de asemenea, că, în conformitate cu propunerea de directivă a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/1148 ([9]) (denumită în continuare „propunerea de directivă NIS2"), „incidentele evitate la limită" ([10]) vor fi supuse obligațiilor de raportare ([11]). În timp ce considerentul (39) al propunerii de directivă NIS2 se referă la sensul termenului „incidente evitate la limită", nu este clar dacă intenția este de a impune raportarea incidentelor evitate la limită de către entitățile financiare enumerate la articolul 2 din propunerea de regulament. În acest sens și ținând seama, de asemenea, de faptul că incidentele evitate la limită pot fi identificate ca atare numai după producerea acestora, BCE ar aprecia primirea în timp util a notificării cu privire la un număr semnificativ de incidente evitate la limită, așa cum se întâmplă în prezent în cazul incidentelor cibernetice. BCE sugerează că ar trebui să existe o mai bună coordonare între regulamentul propus și propunerea de directivă NIS2 pentru a clarifica domeniul exact de raportare la care poate fi supusă orice entitate financiară în temeiul acestor două acte legislative distincte, dar conectate ale Uniunii. În același timp, ar trebui definite „incidentele evitate la limită" și ar trebui elaborate dispoziții care să clarifice semnificația acestora.

1.4 BCE consideră binevenită stimularea entităților financiare să facă schimb, în mod voluntar, de informații secrete privind amenințările cibernetice, pentru a-și consolida și consolida pozițiile în materie de reziliență cibernetică. BCE însăși a contribuit la Inițiativa privind schimbul de informații privind amenințările cibernetice (CIISI-EU), impulsionată de piață, și a pus la dispoziție planurile pentru ca oricine să elaboreze și să promoveze o astfel de inițiativă ([12]).

1.5 BCE sprijină cooperarea dintre autoritățile competente în sensul regulamentului propus, autoritățile europene de supraveghere (AES) și echipele de intervenție în caz de incidente de securitate informatică (CSIRTS) ([13]). Schimbul de informații este esențial pentru a asigura reziliența operațională a Uniunii, întrucât schimbul de informații și cooperarea dintre autorități pot contribui la prevenirea atacurilor cibernetice și la reducerea răspândirii amenințărilor TIC. Ar trebui promovată o înțelegere comună a riscurilor legate de TIC și ar trebui să se asigure o evaluare coerentă a acestor riscuri în întreaga Uniune. Este extrem de important ca informațiile să fie partajate cu punctul unic de contact ([14]) și cu CSIRTS naționale de către autoritățile competente ([15]) numai atunci când există mecanisme de clasificare și de schimb de informații clar stabilite, însoțite de garanții adecvate pentru a asigura confidențialitatea.

1.6 În cele din urmă, BCE consideră binevenită introducerea în propunerea de regulament a unor norme privind datele cu caracter personal și păstrarea datelor. Durata perioadei de păstrare ar trebui să ia în considerare investigarea, inspecția, solicitarea de informații, comunicarea, publicarea, evaluarea, verificarea, aprecierea și elaborarea planurilor de supraveghere sau de monitorizare pe care autoritățile competente ar putea fi nevoite să le efectueze ca parte a obligațiilor și sarcinilor care le revin în temeiul regulamentului propus. În acest sens, o perioadă de păstrare de 15 ani ar fi adecvată. Această perioadă de păstrare a datelor ar putea fi scurtată sau prelungită, după cum o impun anumite situații. În acest sens, BCE sugerează ca organele

([6]) A se vedea articolul 3 alineatul (15) din regulamentul propus.
([7]) A se vedea articolul 31 alineatul (1) litera (d) din regulamentul propus.
([8]) A se vedea articolul 15 alineatul (3) din Directiva NIS.
([9]) COM(2020) 823 final.
([10]) Evenimente care ar fi putut cauza prejudicii, dar a căror desfășurare până la capăt a fost împiedicată cu succes; a se vedea considerentul (39) al Directivei NIS2.
([11]) A se vedea articolul 11 din Directiva NIS2.
([12]) Inițiativa privind schimbul de informații privind amenințările cibernetice (CIISI-EU), disponibilă pe website-ul BCE www.ecb.europa.eu.
([13]) A se vedea articolul 42 din regulamentul propus.
([14]) A se vedea articolul 8 alineatul (3) din Directiva NIS.
([15]) A se vedea, de asemenea, articolele 11, 26 și 27 din Directiva NIS2.

legislative ale Uniunii, atunci când formulează dispoziția relevantă privind datele cu caracter personal și păstrarea datelor, să țină seama, de asemenea, de principiul minimizării datelor, precum și de prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice ([16]).

2. **Observații specifice privind monitorizarea, precum și compensarea și decontarea titlurilor de valoare**

2.1 *Competențele SEBC și ale Eurosistemului în materie de monitorizare*

2.1.1 În strânsă legătură cu misiunile sale de politică monetară de bază, Tratatul și Statutul Sistemului European al Băncilor Centrale și al Băncii Centrale Europene (denumit în continuare „Statutul SEBC") prevăd realizarea de către Eurosistem a monitorizării sistemelor de compensare și de plăți. Conform articolului 127 alineatul (2) a patra liniuță din Tratat, astfel cum este reflectat în articolul 3.1 din Statut, una dintre misiunile fundamentale care să fie îndeplinite prin intermediul Sistemului European al Băncilor Centrale (SEBC) este de a promova buna funcționare a sistemelor de plăți. În îndeplinirea acestei misiuni fundamentale, „BCE și băncile centrale naționale pot acorda facilități, iar BCE poate adopta regulamente în vederea asigurării eficienței și solidității sistemelor de compensare și de plăți în cadrul Uniunii și în raporturile cu țările terțe" ([17]). În temeiul rolului său de monitorizare, BCE a adoptat Regulamentul (UE) nr. 795/2014 al Băncii Centrale Europene (BCE/2014/28) (denumit în continuare „Regulamentul SIPS") ([18]). Regulamentul SIPS pune în aplicare, în formă prescriptivă, Principiile pentru infrastructurile pieței financiare din aprilie 2012, emise de Comitetul pentru sisteme de plăți și decontare și de Organizația Internațională a Comisiilor de Valori Mobiliare ([19]), care sunt obligatorii din punct de vedere juridic și acoperă atât sistemele de plăți de mare valoare, cât și sistemele de plăți de mică valoare de importanță sistemică, operate fie de o bancă centrală din Eurosistem, fie de o entitate privată. Cadrul politicii de monitorizare a Eurosistemului ([20]) identifică instrumentele de plată drept „parte integrantă a sistemelor de plăți" și, prin urmare, le include în sfera monitorizării pe care o face. Cadrul de monitorizare pentru instrumentele de plată este în prezent în curs de revizuire ([21]). În temeiul acestui cadru, un instrument de plată (de exemplu, un card, un transfer de credit, o debitare directă, un transfer de monedă electronică și un token pentru plată digitală ([22])) este definit ca un dispozitiv personalizat (sau un set de dispozitive) și/sau un set de proceduri convenite între utilizatorul serviciilor de plată și prestatorul de servicii de plată utilizat pentru a iniția un transfer de valoare ([23]) .

2.1.2 Având în vedere cele de mai sus, BCE apreciază excluderea din domeniul de aplicare al regulamentului propus a operatorilor de sistem, astfel cum sunt definiți la articolul 2 litera (p) din Directiva 98/26/CE a Parlamentului European și a Consiliului ([24]), a sistemelor de plăți (inclusiv a celor operate de băncile centrale), a schemelor de

([16]) A se vedea articolul 4 litera (b) și articolul 13 din 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)..

([17]) A se vedea articolul 22 din Statutul SEBC.

([18]) Regulamentul (UE) nr. 795/2014 al Băncii Centrale Europene din 3 iulie 2014 privind cerințele de monitorizare pentru sistemele de plăți de importanță sistemică (BCE/2014/28) (JO L 217, 23.7.2014, p. 16).

([19]) Disponibile pe website-ul Băncii Reglementelor Internaționale, la adresa www.bis.org.

([20]) Eurosystem oversight policy framework (Cadrul politicii de monitorizare a Eurosistemului), versiunea revizuită (iulie 2016) disponibilă pe website-ul BCE la adresa www.ecb.europa.eu.

([21]) A se vedea cadrul de monitorizare al Eurosistemului pentru instrumentele, schemele și aranjamentele de plată electronică din octombrie 2020 (cadrul PISA) revizuit și consolidat, disponibil pe website-ul BCE la adresa www.ecb.europa.eu.

([22]) Un token de plată digitală este o reprezentare digitală a valorii garantate cu creanțe sau active înregistrate în altă parte și care permite transferul de valoare între utilizatorii finali. În funcție de conceptul de bază, tokenurile de plată digitală pot prevedea un transfer de valoare fără a implica în mod necesar o parte terță centrală și/sau fără a utiliza conturi de plăți.

([23]) „Transfer de valoare" „Acțiunea, inițiată de plătitor sau în numele plătitorului sau de beneficiarul plății, de a transfera fonduri sau tokenuri de plată digitală sau de a plasa sau retrage numerar într-un/dintr-un cont de utilizator, indiferent de eventualele obligații subiacente existente între plătitor și beneficiarul plății. Transferul poate implica unul sau mai mulți prestatori de servicii de plată." Această definiție a „transferului de valoare" prevăzută în cadrul PISA se îndepărtează de definiția transferului de „fonduri" din 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). Un „transfer de valoare" în contextul unui „instrument de plată", astfel cum este definit în această directivă, se poate referi doar la un transfer de „fonduri". În cadrul acestei directive, „fondurile" nu includ tokenurile de plată digitală, cu excepția cazului în care tokenurile pot fi clasificate drept monedă electronică (sau, mai ipotetic, ca monedă scripturală).

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

plăți și a mecanismelor de plată în vederea aplicării cadrelor de monitorizare menționate mai sus. Din aceste motive, competențele SEBC în temeiul tratatului și competențele Eurosistemului în temeiul Regulamentului SIPS ar trebui să fie clar precizate în considerentele regulamentului propus.

2.1.3 În același sens, BCE apreciază excluderea de la aplicarea cadrului de monitorizare prevăzut în propunerea de regulament a furnizorilor terți de servicii TIC care fac obiectul cadrelor de monitorizare instituite în scopul sprijinirii sarcinilor menționate la articolul 127 alineatul (2) din tratat ([25]). În acest sens, BCE ar dori să sublinieze faptul că băncile centrale din cadrul SEBC care acționează în cadrul capacităților lor monetare ([26]) și Eurosistemul atunci când furnizează servicii prin intermediul TARGET2, TARGET2-Securites (T2S) ([27]) și TARGET Instant Payment Settlement (TIPS) ([28]) nu fac obiectul articolului privind domeniul de aplicare din regulamentul propus și nici nu pot fi considerate furnizori terți de servicii TIC și, prin urmare, nu ar putea fi clasificați drept furnizorilor terți esențiali de servicii TIC în sensul regulamentului propus. Eurosistemul monitorizează T2S în legătură cu mandatul său de a asigura sisteme eficiente și solide de compensare și plăți. În plus, ESMA a clarificat faptul că T2S nu este un furnizor esențial de servicii ([29]) în sensul Regulamentul (UE) nr. 909/2014 al Parlamentului European și al Consiliului ([30]) (denumit în continuare „Regulamentul privind CSD-urile"). Prin urmare, siguranța organizațională și operațională, eficiența și reziliența T2S sunt asigurate prin intermediul cadrului juridic, de reglementare și operațional aplicabil și al mecanismelor de guvernanță convenite sau T2S, iar nu prin intermediul Regulamentului privind CSD-urile.

2.1.4 În plus, cadrul politicii de monitorizare a Eurosistemului ([31]) include furnizorii esențiali de servicii, cum ar fi Societatea de Comunicații Financiare Interbancare Globale (Society for Worldwide Interbank Financial Telecommunication - SWIFT). SWIFT este o societate cooperativă cu răspundere limitată cu sediul în Belgia, care furnizează servicii de mesagerie securizate la nivel internațional. Nationale Bank van België/Banque Nationale de Belgique acționează în calitate de supervizor principal al SWIFT și realizează, pe baza unui acord de monitorizare cooperativă, monitorizarea cu privire la SWIFT, în cooperare cu celelalte bănci centrale din G10, inclusiv cu BCE. Supervizorii din cadrul G10 recunosc că principalul obiectiv al monitorizăriiîl reprezintă riscul operațional al SWIFT, deoarece acesta este considerat a fi principala categorie de risc prin care SWIFT ar putea prezenta un risc sistemic pentru sistemul financiar din Uniune. În acest sens, Grupul de monitorizare cooperativă SWIFT a elaborat un set specific de principii și așteptări la nivel înalt care se aplică SWIFT, cum ar fi identificarea și gestionarea riscurilor, securitatea informațiilor, fiabilitatea și reziliența, planificarea tehnologică și comunicarea cu utilizatorii. Supervizorii G10 se așteaptă ca SWIFT să adere la orientările Comitetului pentru infrastructuri de plăți și de piață (CPMI) și ale Organizației Internaționale a Comisiilor de Valori Mobiliare (IOSCO) privind reziliența cibernetică ([32]), precum și la alte standarde internaționale privind securitatea TIC care, luate împreună, depășesc cerințele stabilite în regulamentul propus.

2.1.5 Nu se poate garanta că SWIFT și poate alți furnizori de servicii care fac obiectul cadrului politicii de monitorizare a Eurosistemului ar putea intra sub incidența regulamentului propus în calitate de furnizori terți de servicii TIC în cazul în care ar furniza servicii care nu intră sub incidența articolului 127 alineatul (2) din tratat. Prin urmare, BCE apreciază foarte mult faptul că furnizorii de servicii care fac deja obiectul cadrului politicii de monitorizare a Eurosistemului, inclusiv, dar fără a se limita la SWIFT, sunt excluși din domeniul de aplicare al cadrului de monitorizare prevăzut în regulamentul propus.

([25]) A se vedea articolul 28 alineatul (5) din regulamentul propus.

([26]) A se vedea punctul 1.3 din Avizul Băncii Centrale Europene din 19 februarie 2021 cu privire la o propunere de regulament privind piețele criptoactivelor și de modificare a Directivei (UE) 2019/1937 (CON/2021/4). Toate avizele BCE se publică pe EUR-Lex.

([27]) A se vedea Anexa IIa la Orientarea BCE/2012/27 a Băncii Centrale Europene din 5 decembrie 2012 privind sistemul transeuropean automat de transfer rapid cu decontare pe bază brută în timp real (TARGET2) (JO L 30, 30.1.2013, p. 1). Orientarea BCE/2012/13 a Băncii Centrale Europene din 18 iulie 2012 privind TARGET2-Securities (JO L 215, 11.8.2012, p. 19); și Decizia BCE/2011/20 a Băncii Centrale Europene din 16 noiembrie 2011 de stabilire a normelor detaliate și a procedurilor de punere în aplicare a criteriilor de eligibilitate pentru accesul depozitarilor centrali de valori mobiliare la serviciile TARGET2-Securities (JO L 319, 2.12.2011, p. 117). A se vedea, de asemenea, Acordul-cadru și Convenția colectivă privind T2S.

([28]) A se vedea anexa IIb la Orientarea BCE/2012/27.

([29]) A se vedea articolul 30 alineatul (5) din 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 (OJ L 257, 28.8.2014, p. 1), precum și articolul 68 din Regulamentul delegat (UE) nr. 2017/392 al Comisiei din 11 noiembrie 2016 de completare a Regulamentului (UE) nr. 909/2014 al Parlamentului European și al Consiliului cu privire la standarde tehnice de reglementare în materie de autorizare, supraveghere și cerințe operaționale pentru depozitarii centrali de titluri de valoare (JO L 65, 10.3.2017, p. 48)

([30]) 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).

([31]) Eurosystem oversight policy framework (Cadrul politicii de monitorizare a Eurosistemului), versiunea revizuită (iulie 2016) disponibilă pe website-ul BCE la adresa www.ecb.europa.eu.

([32]) Disponibile pe website-ul Băncii Reglementelor Internaționale, la adresa www.bis.org.

2.2 *Competențele SEBC în domeniul decontării titlurilor de valoare*

2.2.1 Depozitarii centrali de titluri de valoare (CSD-urile) sunt infrastructuri ale pieței financiare (IPF) care sunt strict reglementate și supravegheate de diferite autorități în temeiul Regulamentului privind CSD-urile, care stabilește cerințe privind decontarea instrumentelor financiare, precum și norme privind organizarea și conduita CSD-urilor. În plus, CSD-urile ar trebui să ia act de Orientările CPMI-IOSCO privind reziliența cibernetică, care au fost operaționalizate prin Așteptările în materie de monitorizare în ceea ce privește reziliența cibernetică, care sunt aplicate infrastructurilor piețelor financiare (decembrie 2018) ([33]) . Pe lângă competențele de supraveghere încredințate autorităților naționale competente (ANC) în temeiul Regulamentului privind CSD-urile, membrii SEBC acționează drept „autorități relevante", în calitatea lor de autorități de monitorizare ai sistemelor de plăți și de decontare a titlurilor de valoare gestionate de CSD-uri, de bănci centrale care emit cele mai relevante monede în care are loc decontarea și de bănci centrale în ale căror registre se decontează segmentul aferent fondurilor bănești al tranzacțiilor ([34]). În acest sens, considerentul 8 din Regulamentul privind CSD-urile prevede că regulamentul ar trebui să se aplice fără a aduce atingere responsabilităților BCE și ale băncilor centrale naționale de a asigura sisteme de compensare și sisteme de plăți eficiente și solide în Uniune și în alte țări. Considerentul (8) prevede, de asemenea, că Regulamentul privind CSD-urile nu ar trebui să împiedice membrii SEBC să acceseze informații relevante pentru îndeplinirea sarcinilor lor ([35]), inclusiv pentru monitorizarea CSD-urilor și a altor IPF-uri ([36]).

2.2.2 În plus, membrii SEBC acționează adesea ca agenți de decontare pentru segmentul aferent fondurilor bănești al tranzacțiilor cu titluri de valoare, iar Eurosistemul oferă servicii de decontare prin T2S către CSD. Monitorizarea T2S de către Eurosistem este legată de mandatul său de a asigura sisteme de compensare și de plăți eficiente și solide, în timp ce autoritățile competente și relevante ale CSD-urilor urmăresc să asigure buna funcționare a acestora, siguranța și eficiența decontării și funcționarea corespunzătoare a piețelor financiare în jurisdicțiile lor respective.

2.2.3 Potrivit regulamentului propus ([37]), băncile centrale din cadrul SEBC nu sunt implicate în elaborarea de standarde tehnice în ceea ce privește specificarea riscurilor TIC. În mod similar, în temeiul regulamentului propus ([38]), autoritățile competente nu sunt informate cu privire la incidente legate de TIC. Banca centrală din cadrul SEBC ar trebui să mențină același nivel de implicare ca cel prevăzut în prezent în Regulamentul privind CSD-urile, iar autoritățile relevante ar trebui să fie informate cu privire la incidentele legate de TIC. Eurosistemul este autoritatea relevantă pentru toate CSD-urile din zona euro și pentru alte câteva CSD-uri din UE. Băncile centrale din cadrul SEBC ar trebui să fie informate cu privire la incidentele legate de TIC care sunt relevante pentru îndeplinirea sarcinilor lor, inclusiv monitorizarea CSD-urilor și a altor IPF-uri. Riscurile la care sunt expuse CSD-urile, inclusiv riscurile TIC, au potențialul de a amenința buna funcționare a CSD-urilor. Prin urmare, riscurile privind TIC sunt importante pentru autoritățile relevante, care ar trebui să primească o prezentare completă și detaliată cu privire la aceste riscuri pentru a le evalua și pentru a influența abordarea privind gestionarea riscurilor adoptată de CSD-uri. Regulamentul propus nu ar trebui să prevadă cerințe mai puțin restrictive în ceea ce privește riscurile privind TIC în comparație cu cele prevăzute în Regulamentul privind CSD-urile și în actualele standarde tehnice de reglementare conexe.

2.2.4 În plus, organele legislative ale Uniunii ar trebui să clarifice interacțiunea dintre regulamentul propus ([39]) și standardele tehnice de reglementare care completează Regulamentul privind CSD-urile. În special, nu este clar dacă un CSD trebuie să fie scutit de obligația de a avea propriul sediu secundar în care furnizorul său de servicii TIC terț are un astfel de sediu ([40]). În cazul în care un CSD este scutit de această obligație de a menține

([33]) Disponibil pe website-ul BCE, la adresa: www.ecb.europa.eu.

([34]) A se vedea articolul 12 din Regulamentul (UE) nr. 909/2014.

([35]) A se vedea, de asemenea, articolele 13, 17 alineatul (4) și 22 alineatul (6) din Regulamentul (UE) nr. 909/2014.

([36]) A se vedea punctul 7.3 din Avizul Băncii Centrale Europeni din 6 aprilie 2017 cu privire la infrastructura Critice în domeniul securității informațiilor (CON/2017/10); punctul 7.2 din Avizul Băncii Centrale Europene din 8 noiembrie 2018 privind desemnarea serviciilor esențiale și a operatorilor de servicii esențiale în scopul securității rețelelor și a sistemelor informatice (CON/2018/47); punctul 3.5.2 din Avizul Băncii Centrale Europene din 2 mai 2019 privind securitatea rețelelor și a sistemelor informatice (CON/2019/17); și punctul 3.5.2 din Avizul Băncii Centrale Europene din 11 noiembrie 2019 privind securitatea rețelelor și a sistemelor informatice (CON/2019/38).

([37]) A se vedea articolul 54 alineatul (5) din regulamentul propus și articolul 45 alineatul (7) din Regulamentul (UE) nr. 909/2014.

([38]) A se vedea articolul 54 alineatul (4) din regulamentul propus și articolul 45 alineatul (6) din Regulamentul (UE) nr. 909/2014.

([39]) A se vedea articolul 11 alineatul (5) din regulamentul propus.

([40]) A se vedea articolul 78 alineatul (3) din Regulamentul delegat (UE) nr. 2017/392 al Comisiei din 11 noiembrie 2016 de completare a Regulamentului (UE) nr. 909/2014 al Parlamentului European și al Consiliului cu privire la standarde tehnice de reglementare în materie de autorizare, supraveghere și cerințe operaționale pentru depozitarii centrali de titluri de valoare (JO L 65, 10.3.2017, p. 48).

un sediu secundar, nu este clar care ar fi valoarea juridică pe care ar avea-o această cerință. În aceeași ordine de idei, regulamentul propus ([41]) se referă la un obiectiv privind durata recuperării și la obiective privind momentul recuperării pentru fiecare funcție ([42]), în timp ce standardul tehnic de reglementare relevant face o distincție între funcțiile esențiale ([43]) și operațiunile esențiale ([44]) în raport cu durata recuperării stabilite pentru operațiunile esențiale ale CSD-urilor. Sunt necesare clarificări și reflecții suplimentare din partea organelor legislative ale Uniunii cu privire la interacțiunea dintre regulamentul propus și standardele tehnice de reglementare care completează Regulamentul privind CSD-urile, pentru a evita riscul unor cerințe contradictorii. În cele din urmă, ar trebui clarificat faptul că derogările acordate CSD-urilor gestionate de anumite entități publice în temeiul Regulamentului privind CSD-urile ([45]) sunt extinse prin regulamentul propus.

2.3 *Competențele SEBC în domeniul compensării titlurilor de valoare*

2.3.1 Băncilor centrale din cadrul SEBC le sunt încredințate competențe de monitorizare în ceea ce privește contrapartidele centrale (CPC). În acest sens, băncile centrale naționale din Eurosistem cooperează adesea cu autoritățile naționale competente relevante în ceea ce privește funcțiile de supraveghere și de monitorizare a CPC-urilor și participă la colegiul CPC respectiv instituit în temeiul Regulamentului (UE) nr. 648/2012 al Parlamentului European și al Consiliului ([46]) (denumit în continuare „EMIR"). Membrii relevanți ai Eurosistemului ([47]) participă la colegiile EMIR în calitatea lor autorități de monitorizare și reprezintă Eurosistemul ca bancă centrală de emisiune pentru CPC în cazul cărora euro este una dintre cele mai relevante monede pentru instrumentele financiare compensate (și pentru CPC-urile offshore care compensează o proporție semnificativă de instrumente financiare în euro). BCE este banca centrală de emisiune pentru CPC din afara zonei euro.

2.3.2 Potrivit regulamentului propus ([48]), băncile centrale din cadrul SEBC nu sunt implicate în elaborarea de standarde tehnice în ceea ce privește specificarea riscurilor TIC. În plus, regulamentul propus ([49]) nu conține nicio trimitere la obiectivul privind durata recuperării și la cerințele privind obiectivul privind momentul recuperării în temeiul EMIR ([50]). Cadrul de reglementare propus nu ar trebui să prevadă cerințe mai puțin restrictive în ceea ce privește riscurile privind TIC decât cele existente în prezent. Prin urmare, este esențial să se stabilească obiective clare privind durata și momentul recuperării pentru a avea un cadru solid de gestionare a continuității activității. Menținerea unor obiective specifice privind durata și momentul recuperării face parte, de asemenea, din Principiile CPMI-IOSCO pentru infrastructurile pieței financiare ([51]). Dispoziția actuală din EMIR ar trebui menținută, iar regulamentul propus ar trebui adaptat în consecință. Băncile centrale din cadrul SEBC ar trebui să fie implicate în pregătirea oricărei legislații de nivel secundar, precum și în clarificări și reflecții suplimentare din partea organelor legislative ale Uniunii cu privire la interacțiunea dintre regulamentul propus și standardele tehnice de reglementare de completare, astfel încât să se evite riscul unor cerințe contradictorii sau suprapuse.

3. **Observații specifice privind aspectele legate de supravegherea prudențială**

3.1 Regulamentul (UE) nr. 1024/2013 al Consiliului ([52]) (denumit în continuare „Regulamentul privind MUS") conferă BCE atribuții specifice în ceea ce privește supravegherea prudențială a instituțiilor de credit din zona euro și conferă BCE responsabilitatea pentru funcționarea eficace și consecventă a mecanismului unic de supraveghere (MUS), în cadrul căruia responsabilitățile specifice în materie de supraveghere prudențială sunt repartizate între BCE și ANC participante. În special, BCE îndeplinește atribuția de a autoriza și de a retrage autorizațiile tuturor instituțiilor de credit . BCE are, de asemenea, sarcina, printre altele, de a asigura conformitatea cu legislația relevantă a Uniunii care impune instituțiilor de credit cerințe prudențiale, inclusiv cerința de a dispune de mecanisme de guvernanță solide, cum ar fi procese solide de gestionare a riscurilor și mecanisme de control intern ([53]). În acest scop, BCE dispune de

([41]) A se vedea articolul 11 alineatul (6) din regulamentul propus.
([42]) A se vedea articolul 3 alineatul (17) din regulamentul propus.
([43]) A se vedea articolul 76 alineatul (2) litera (d) și litera (e) din Regulamentul delegat (UE) nr. 2017/392 al Comisiei.
([44]) A se vedea articolul 78 alineatele (2) și (3) din Regulamentul delegat (UE) nr. 2017/392 al Comisiei.
([45]) A se vedea articolul 1 alineatul (4) din Regulamentul (UE) nr. 909/2014.
([46]) 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).
([47]) A se vedea articolul 18 alineatul (2) litera (g) și litera (h) din EMIR.
([48]) A se vedea articolul 53 alineatul (2) litera (b) și articolul 53 alineatul (3) din regulamentul propus și articolul 34 alineatul (3) din EMIR.
([49]) A se vedea articolul 53 alineatul (2) litera (a) din regulamentul propus.
([50]) A se vedea articolul 34 din EMIR.
([51]) A se vedea CPMI-IOSCO Principles for Financial Market Infrastructures (Principiile CPMI-IOSCO pentru infrastructurile pieței financiare) disponibile pe website-ul Băncii Reglementelor Internaționale: www.bis.org.
([52]) 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).
([53]) A se vedea articolul 4 alineatul (1) litera (e) și articolul 6 alineatul (4) din Regulamentul (UE) nr. 1024/2013.

toate competențele de supraveghere necesare pentru a interveni în activitatea instituțiilor de credit pentru exercitarea funcțiilor sale. Prin urmare, BCE și ANC relevante sunt autoritățile competente care exercită competențe specifice de supraveghere prudențială în temeiul Regulamentului 2013/575/UE al Parlamentului European și al Consiliulu ([54]) (denumit în continuare „Regulamentul privind cerințele de capital") și al Directivei 2013/36/UE a Parlamentului European și a Consiliului ([55]) (denumită în continuare „Directiva privind cerințele de capital").

3.2 Regulamentul propus prevede că setul unic de norme și sistemul de supraveghere ar trebui dezvoltate în continuare pentru a include reziliența operațională digitală și securitatea TIC, prin extinderea mandatelor autorităților de supraveghere financiară însărcinate cu monitorizarea și protejarea stabilității financiare și a integrității pieței ([56]). Scopul este de a promova un cadru cuprinzător pentru riscurile privind TIC sau operaționale prin armonizarea cerințelor esențiale privind reziliența operațională digitală pentru toate entitățile financiare ([57]). În special, regulamentul propus vizează consolidarea și actualizarea cerințelor privind riscurile privind TIC care, în prezent, sunt abordate separat în diferite acte legislative ([58]).

3.3 Cerințele legate de riscul privind TIC pentru sectorul financiar sunt în prezent dispersate într-o serie de acte legislative ale Uniunii, inclusiv Directiva privind cerințele de capital, și de instrumente juridice neobligatorii (cum ar fi orientările ABE) și sunt diverse și uneori incomplete. În unele cazuri, riscul privind TIC a fost abordat doar implicit ca parte a riscului operațional, în timp ce în alte cazuri nu a fost abordat deloc. Acest lucru ar trebui remediat prin alinierea regulamentului propus cu actele respective. În acest scop, directiva de modificare propusă prezintă o serie de modificări care par necesare pentru a asigura claritatea și coerența juridică în ceea ce privește aplicarea diferitelor cerințe privind reziliența operațională digitală. Cu toate acestea, modificările la Directiva privind cerințele de capital sugerate în prezent de directiva de modificare propusă ([59]) se referă doar la dispozițiile privind planurile de urgență și de asigurare a continuității activității ([60]), având în vedere că acestea ar servi implicit drept bază pentru abordarea gestionării riscurilor TIC.

3.4 În plus, regulamentul propus ([61]) prevede că entitățile financiare, inclusiv instituțiile de credit, trebuie să dispună de cadre interne de guvernanță și control care să asigure o gestionare eficace și prudentă a tuturor riscurilor TIC. Regulamentul propus ([62]) prevede aplicarea la nivel individual și consolidat a cerințelor stabilite în acesta, dar fără o coordonare suficientă cu legislația sectorială specifică menționată. În sfârșit, în regulamentului propus ([63]), se prevede că, fără a aduce atingere dispozițiilor privind cadrul de monitorizare pentru furnizorii terți esențiali de servicii TIC menționați în regulamentul propus ([64]), respectarea obligațiilor prevăzute în regulamentul respectiv este asigurată, pentru instituțiile de credit, de către autoritatea competentă desemnată în conformitate cu articolul 4 din Directiva privind cerințele de capital, fără a aduce atingere atribuțiilor specifice conferite BCE prin Regulamentul privind MUS.

3.5 Având în vedere cele de mai sus, BCE înțelege că, în ceea ce privește instituțiile de credit și cu excepția dispozițiilor regulamentului propus referitoare la cadrul de monitorizare pentru furnizorii terți esențiali de servicii TIC ([65]), regulamentul propus intenționează să stabilească un cadru de guvernanță internă prudențială pentru gestionarea riscurilor TIC, care va fi integrat în cadrul general de guvernanță internă stabilit prin Directiva privind cerințele de capital. În plus, având în vedere natura prudențială a cadrului propus, autoritățile competente responsabile cu supravegherea respectării obligațiilor prevăzute în cadrul propus, inclusiv BCE, vor fi autoritățile responsabile cu supravegherea bancară în conformitate cu Regulamentul privind MUS.

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

([55]) 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 și a firmelor de investiții, 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).

([56]) A se vedea considerentul (8) al regulamentului propus.

([57]) A se vedea considerentul (11) al regulamentului propus.

([58]) A se vedea considerentul (12) al regulamentului propus.

([59]) A se vedea considerentele (4) și (5) ale directivei de modificare propuse.

([60]) A se vedea articolul 85 din Directiva privind cerințele de capital.

([61]) A se vedea articolul 4 alineatul (1) din regulamentul propus.

([62]) A se vedea articolul 25 alineatele (3) și (4) din regulamentul propus.

([63]) A se vedea articolul 41 din regulamentul propus.

([64]) A se vedea capitolul V secțiunea II din regulamentul propus.

([65]) A se vedea capitolul V secțiunea II din regulamentul propus.

3.6 Prin urmare, organele legislative ale Uniunii ar putea dori să ia în considerare următoarele sugestii pentru a spori claritatea și coordonarea între regulamentul propus și Directiva privind cerințele de capital. În primul rând, cerințele din regulamentul propus pot fi calificate în mod expres drept prudențiale, astfel cum s-a procedat, printre altele, în Regulamentul privind CSD-urile ([66]). În al doilea rând, considerentele directivei de modificare propuse ([67]) ar putea extinde formularea acestora, având în vedere că cerințele din regulamentul propus depășesc simpla fază a planurilor de urgență și de asigurare a continuității activității. Măsurile de guvernanță a riscurilor privind TIC intră, în general, în domeniul de aplicare mai general al unor mecanisme solide de guvernanță în temeiul articolului 74 din Directiva privind cerințele de capital ([68]). În al treilea rând, regulamentul propus ([69]) ar trebui modificat pentru a reaminti în considerente competența BCE în ceea ce privește supravegherea prudențială a instituțiilor de credit în temeiul tratatului și al Regulamentului privind MUS. În al patrulea rând, trimiterea la aplicarea la nivel individual și consolidat a cerințelor prevăzute în acesta ([70]) ar trebui revizuită, deoarece nivelul subconsolidat și cel consolidat nu sunt definite în regulamentul propus iar anumite tipuri de intermediari nu fac obiectul supravegherii consolidate în temeiul legislației relevante (de exemplu, instituțiile de plată). În plus, nivelul de aplicare a cerințelor din regulamentul propus ar trebui să decurgă exclusiv din legislația aplicabilă fiecărui tip de entitate financiară. În cazul instituțiilor de credit, este prevăzută o legătură clară între Directiva privind cerințele de capital și regulamentul propus și, prin urmare, cerințele din regulamentul propus s-ar aplica automat la nivel individual, subconsolidat sau consolidat ([71]), după caz. În cele din urmă, organele legislative ale Uniunii ar putea lua în considerare posibilitatea de a prevedea un regim tranzitoriu pentru gestionarea perioadei cuprinse între intrarea în vigoare a regulamentului propus și intrarea în vigoare a standardelor tehnice de reglementare prevăzute în regulamentul propus, având în vedere că unii intermediari, inclusiv instituțiile de credit, fac deja obiectul unor norme privind riscurile privind TIC aplicabile anumitor sectoare și care sunt mai detaliate decât dispozițiile generale ale regulamentului propus.

3.7 În temeiul Regulamentului privind MUS, BCE a primit sarcina de a asigura respectarea de către instituțiile de credit a cerințelor dreptului Uniunii care impun instituțiilor de credit să dispună de procese solide de gestionare a riscurilor și de mecanisme de control intern ([72]). Aceasta înseamnă că BCE trebuie să se asigure că instituțiile de credit aplică politici și procese de evaluare și administrare a expunerii lor la riscul operațional, inclusiv la riscul de model și care acoperă evenimentele deosebit de grave și cu o frecvență redusă. Instituțiile de credit au obligația de a stabili ceea ce reprezintă risc operațional în sensul acestor politici și proceduri ([73]).

3.8 În luna iulie 2017, Consiliul guvernatorilor Băncii Centrale Europene (BCE) a adoptat Cadrul MUS de raportare a incidentelor cibernetice (denumit în continuare „cadrul"), pe baza unui proiect de propunere a Consiliului de supraveghere în conformitate cu articolul 26 alineatul (8) și cu articolul 6 alineatul (2) din Regulamentul privind MUS și cu articolul 21 alineatul (1) din Regulamentul (UE) nr. 468/2014 al Băncii Centrale Europene (BCE/2014/17) ([74]). Cadrul constă într-o cerere care produce efecte juridice (decizii individuale adresate instituțiilor de credit) de informare și/sau raportare în temeiul articolului 10 din Regulamentul privind MUS ([75]). Unele țări dispun deja de un proces de raportare a incidentelor, care impune instituțiilor de credit să raporteze ANC toate incidentele cibernetice semnificative. În aceste țări, instituțiile de credit semnificative vor raporta în continuare incidentele către ANC, care le va transmite ulterior, fără întârzieri nejustificate, BCE în numele entităților supravegheate. Prin urmare, deciziile menționate mai sus se adresează, de asemenea, acestor autorități naționale

([66]) A se vedea titlul capitolului II secțiunea 4 „Cerințe prudențiale" din Regulamentul privind CSD-urile.

([67]) A se vedea considerentul (4) al directivei de modificare propuse.

([68]) Articolul 85 din Directiva 2013/36/UE constituie o simplă specificație. În acest sens, a se vedea, de asemenea, paginile 4, 11 și 37 din Ghidul Autorității bancare europene din 29 noiembrie 2019 privind administrarea riscurilor privind TIC și de securitate (denumit în continuare „Ghidul ABE"), pentru care temeiul juridic general se regăsește în mod expres la articolul 74 din Directiva 2013/36/UE.

([69]) A se vedea articolul 41 alineatul (1) din regulamentul propus.

([70]) A se vedea articolul 25 alineatele (3) și (4) din regulamentul propus.

([71]) A se vedea de asemenea articolul 109 din Directiva privind cerințele de capital.

([72]) A se vedea articolul 4 alineatul (1) litera (e) din Regulamentul privind MUS.

([73]) A se vedea articolul 85 din Directiva privind cerințele de capital.

([74]) Regulamentul (UE) nr. 468/2014 al Băncii Centrale Europene din 16 aprilie 2014 de instituire a cadrului de cooperare la nivelul Mecanismului unic de supraveghere între Banca Centrală Europeană și autoritățile naționale competente și cu autoritățile naționale desemnate (Regulamentul-cadru privind MUS) (BCE/2014/17) (JO L 141, 14.5.2014, p. 1).

([75]) În mod specific, un incident cibernetic – mai exact, o posibilă încălcare identificată a securității informațiilor (fie că este rău intenționată, fie că este accidentală) – trebuie raportat BCE dacă este îndeplinită cel puțin una dintre următoarele condiții: (1) există un posibil impact financiar de 5 milioane EUR sau de 0,1% din CET1; (2) incidentul este raportat public sau aduce prejudicii reputației; (3) incidentul a fost raportat șefului departamentului informatic în afara raportării periodice; (4) banca a notificat incidentul echipei de răspuns la incidente de securitate cibernetică/echipei de intervenție în caz de incidente de securitate informatică, unei agenții de securitate sau poliției; (5) au fost declanșate procedurile de recuperare sau de continuitate a activității în caz de dezastru ori a fost depusă o cerere de despăgubire pentru cazurile de atacuri cibernetice; (6) a existat o încălcare a cerințelor juridice sau de reglementare; sau (7) banca recurge la criterii interne și la aprecierea experților (inclusiv un posibil impact sistemic) și decide să informeze BCE.

competente pentru a transmite aceste informații către BCE pe baza cadrului. BCE sprijină eforturile organelor legislative ale Uniunii de a promova armonizarea și raționalizarea, printre altele, în ceea ce privește setul de norme și obligații aplicabile instituțiilor de credit în ceea ce privește raportarea incidentelor. Având în vedere cele de mai sus, BCE este pregătită să modifice (și, eventual, să abroge) cadrul, dacă este necesar, având în vedere eventuala adoptare a regulamentului propus.

4. **Observații specifice privind gestionarea riscurilor TIC, raportarea incidentelor, testarea rezilienței operaționale și riscurile privind TIC generate de părți terțe**

4.1 *Gestionarea riscurilor TIC*

4.1.1 BCE consideră binevenită introducerea prin regulamentul propus a unui cadru solid și cuprinzător de gestionare a riscurilor TIC, care cuprinde Orientările CPMI-IOSCO privind reziliența cibernetică și este aliniat îndeaproape la cele mai bune practici, inclusiv la perspectivele Eurosistemului de monitorizare cibernetică pentru IPF-uri.

4.1.2 BCE sprijină ideea că entitățile financiare ar trebui să efectueze evaluări ale riscurilor la fiecare „schimbare majoră" la nivelul rețelei și al infrastructurii sistemului informatic ([76]). Acestea fiind spuse, regulamentul propus nu conține nicio definiție a „modificării majore", creând o marjă de manevră nedorită pentru interpretări divergente din partea entităților financiare, care ar putea, în cele din urmă, să împiedice obiectivele de armonizare urmărite de regulamentul propus. Din motive de securitate juridică, organele legislative ale Uniunii ar putea dori să ia în considerare introducerea unei definiții a „modificării majore" în regulamentul propus.

4.1.3 În general, BCE sprijină ideea potrivit căreia entitățile financiare, altele decât microîntreprinderile, trebuie să raporteze autorităților competente costurile și pierderile relevante cauzate de perturbările TIC și de incidentele legate de TIC ([77]). Cu toate acestea, pentru a asigura eficacitatea globală a sistemului și pentru a evita posibilitatea ca autoritățile competente și entitățile financiare să fie copleșite de un număr excesiv de rapoarte, introducerea unor praguri relevante, eventual de natură cantitativă, ar putea fi explorată în mod util de către organele legislative ale Uniunii.

4.1.4 BCE recunoaște posibilitatea ca entitățile financiare să delege unor întreprinderi intragrup sau unor întreprinderi externe sarcinile de verificare a conformității cu cerințele de gestionare a riscurilor TIC, cu aprobarea autorităților competente ([78]). În același timp, este important ca organele legislative ale Uniunii să clarifice modul în care ar urma să fie acordată aprobarea de către autoritățile competente în cazurile în care o entitate financiară intră în sfera de competență a mai multor autorități competente. Acest lucru s-ar putea întâmpla în cazul în care o entitate financiară este o instituție de credit, un furnizor de servicii de criptoactive și/sau un furnizor de servicii de plată. În cele din urmă, în ceea ce privește identificarea și clasificarea care trebuie efectuată de entitățile financiare în temeiul regulamentului propus ([79]), BCE ar considera prudent, în scopul clasificării activelor, ca regulamentul propus să impună, de asemenea, entităților financiare să țină seama de caracterul esențial al acestor active (și anume, dacă acestea sprijină funcțiile esențiale).

4.2 *Raportarea incidentelor*

4.2.1 BCE apreciază eforturile prezentate în regulamentul propus de armonizare a peisajului de raportare a incidentelor privind TIC în cadrul Uniunii și de a depune eforturi în vederea unei raportări centralizate a incidentelor majore legate de TIC ([80]). Introducerea unui cadru armonizat pentru raportarea incidentelor majore legate de TIC ([81]) către autoritățile competente relevante ar raționaliza și ar armoniza, în principiu, sarcina de raportare a entităților financiare, inclusiv a instituțiilor de credit. Autoritățile competente ar beneficia de pe urma extinderii domeniului de aplicare al incidentelor acoperite, mergând dincolo de incidentele legate de domeniul cibernetic reglementate în prezent de cadrele existente ([82]). Viitoarea adoptare a regulamentului propus ar necesita revizuirea și posibila abrogare a cadrelor existente, inclusiv a cadrului MUS de raportare a incidentelor cibernetice. Acestea fiind spuse, pentru a realiza o raționalizare reală și o aliniere deplină în toate cadrele, este esențial să se asigure că domeniul de aplicare al dispozițiilor privind raportarea incidentelor din cadrul regulamentului propus, inclusiv toate definițiile, pragurile și parametrii de raportare relevanți, este pe deplin aliniat la cadrele relevante. În special, este extrem de

([76]) A se vedea articolul 7 alineatul (3) din regulamentul propus.
([77]) A se vedea articolul 10 alineatul (9) din regulamentul propus.
([78]) A se vedea articolul 5 alineatul (10) din regulamentul propus.
([79]) A se vedea articolul 7 din regulamentul propus.
([80]) A se vedea articolul 19 din regulamentul propus.
([81]) A se vedea articolul 3 alineatul (7), articolul 17 și articolul 18 din regulamentul propus.
([82]) A se vedea de exemplu cadrul.

important să se asigure alinierea între, pe de o parte, regulamentul propus și, pe de altă parte, Directiva (UE) 2015/2366 a Parlamentului European și a Consiliului ([83]) (denumită în continuare „PSD2") și Ghidul ABE privind raportarea incidentelor majore (denumit în continuare „Ghidul ABE"). Directiva de modificare propusă ([84]) conține modificări ale PSD2 în ceea ce privește delimitarea raportării incidentelor între regulamentul propus și PSD2, care ar afecta în principal furnizorii de servicii de plată, care ar putea fi autorizați și ca instituții de credit, precum și autoritățile competente. Există o lipsă de claritate în ceea ce privește procesul de notificare a incidentelor și există o posibilă suprapunere între unele dintre incidentele care trebuie raportate atât în temeiul regulamentului propus, cât și în temeiul Ghidului ABE.

4.2.2 Procedurile de notificare a incidentelor majore în temeiul regulamentului propus ([85]), al PSD2 și, respectiv, al Ghidului ABE corespunzător ar obliga furnizorii de servicii de plată să prezinte autorității lor competente un raport privind incidentul după clasificarea incidentului. De fapt, rapoartele inițiale nu surprind esența, cauza sau zona funcțională afectată de incident, iar furnizorii de servicii de plată pot fi în măsură să facă astfel de distincții numai într-o etapă ulterioară, atunci când devin disponibile informații mai detaliate cu privire la incident. Prin urmare, rapoartele inițiale privind incidentele ar putea fi transmise atât în temeiul regulamentului propus, cât și în temeiul Ghidului ABE sau furnizorii de servicii de plată pot decide cu privire la un cadru unic de raportare și își pot corecta raportările la o dată ulterioară. Aceeași incertitudine (în ceea ce privește, de exemplu, cauza principală a oricărui incident) poate fi reflectată și în rapoartele intermediare și finale. Acest lucru ar spori din nou posibilitatea transmiterii în paralel a rapoartelor către autoritățile competente în temeiul regulamentului propus și al PSD2.

4.2.3 Unele incidente care pot fi clasificate drept incidente legate de TIC pot avea, de asemenea, un impact asupra altor domenii și, prin urmare, ar trebui notificate în conformitate cu Ghidul ABE. Acesta poate fi cazul în care un incident are un impact din perspectiva TIC, dar, în același timp, a afectat, de asemenea, furnizarea de servicii de plată direct și/sau alte domenii sau canale funcționale non-TIC. În plus, ar putea exista situații în care nu este posibil să se facă distincția între incidentele operaționale și cele legate de TIC. În plus, în cazul în care aceeași entitate financiară este o instituție de credit semnificativă și un furnizor de servicii de plată, în temeiul regulamentului propus, aceeași entitate ar trebui să raporteze de două ori incidentul legat de TIC, fiind supusă obligației de raportare față de două autorități competente. Având în vedere cele de mai sus, regulamentul propus ar trebui să precizeze mai clar modul în care interacțiunea dintre PSD2 și Ghidul ABE ar trebui să opereze în practică. Mai mult, din motive de armonizare și raționalizare a obligațiilor de raportare, ar fi important ca organele legislative ale Uniunii să reflecteze asupra aspectelor reziduale ale dublei raportări și să clarifice dacă regulamentul propus, pe de o parte, și PSD2 și Ghidul ABE, pe de altă parte, ar coexista sau dacă ar trebui să existe un set unic de cerințe de raportare a incidentelor.

4.2.4. Regulamentul propus introduce o cerință ca autoritățile competente ([86]), la primirea unui raport, să confirme primirea notificării și să furnizeze entității financiare, în cel mai scurt timp posibil, toate observațiile sau îndrumările necesare, în special pentru a discuta măsurile de remediere la nivelul entității sau modalitățile de a reduce la minimum impactul negativ la nivelul tuturor sectoarelor. Aceasta ar însemna că autoritățile competente ar trebui să contribuie activ la gestionarea și remedierea incidentelor, evaluând, în același timp, și răspunsul unei entități supravegheate la incidentele critice. BCE subliniază că responsabilitatea pentru remedierea și consecințele unui incident ar trebui să rămână în mod clar și exclusiv în sarcina entității financiare în cauză. Prin urmare, BCE ar propune limitarea observațiilor și a îndrumărilor la observațiile și îndrumările prudențiale la nivel înalt. Dacă sfera observațiilor ar fi mai largă, ar fi nevoie de profesioniști specializați cu cunoștințe tehnice foarte substanțiale care nu sunt disponibili în mod obișnuit în rezerva de talente aflată la dispoziția autorităților prudențiale.

4.3 *Testarea rezilienței operaționale digitale*

4.3.1 BCE consideră binevenite cerințele stabilite în regulamentul propus ([87]) privind testarea rezilienței operaționale digitale în rândul entităților financiare și necesitatea ca fiecare instituție să aibă propriul program de testare. Regulamentul propus ([88]) descrie diferitele tipuri de teste ca fiind indicatoare pentru entitățile financiare. Tipurile de teste nu sunt foarte clare, iar unele teste, cum ar fi testele de compatibilitate, chestionarele sau testele bazate pe scenarii, pot face obiectul interpretării de către AES, autoritățile competente sau entitățile financiare. În plus, nu

([83]) 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).

([84]) A se vedea articolul 7 alineatul (9) din directiva de modificare propusă.

([85]) A se vedea articolul 17 alineatul (3) din regulamentul propus.

([86]) A se vedea articolul 20 din regulamentul propus.

([87]) A se vedea articolele 21 și 22 din regulamentul propus.

([88]) A se vedea articolul 22 alineatul (1) din regulamentul propus.

există orientări cu privire la frecvența fiecărui test. O posibilă abordare ar putea fi ca regulamentul propus să stabilească cerințe generice de testare, o descriere mai precisă a tipurilor de teste fiind prevăzută în standardele tehnice de reglementare și de punere în aplicare.

4.3.2 Testele de penetrare bazate pe amenințări (Threat-led penetration testing — TLPT) reprezintă un instrument puternic de testare a apărării și pregătirii în materie de securitate. Prin urmare, BCE încurajează utilizarea TLPT de către entitățile financiare. Cu acest instrument sunt testate nu numai măsurile tehnice, ci și personalul și procesele. Rezultatele acestor teste pot spori semnificativ gradul de conștientizare în materie de securitate a personalului de conducere de nivel superior din cadrul entităților testate. Cadrul european pentru atacul etic bazat pe informații privind amenințările (TIBER-EU) ([89]) și alte instrumente TLPT deja disponibile, în afara Uniunii, sunt instrumente principale pentru ca entitățile înseși să își evalueze, să testeze, să practice și să își îmbunătățească poziția și mijloacele de apărare în materie de reziliență cibernetică.

4.3.3 În majoritatea statelor membre în care a fost pus în aplicare TIBER-UE, autoritățile de monitorizare și cele de supraveghere nu joacă un rol activ în punerea în aplicare a unui program ITBER-XX localizat, iar echipa informatică TIBER (TCT) este în aproape toate cazurile independentă de aceste funcții. Din acest motiv, testarea avansată în temeiul regulamentului propus ([90]), prin intermediul TLPT, ar trebui să fie pusă în aplicare ca instrument de consolidare a ecosistemului financiar și de consolidare a stabilității financiare, mai degrabă decât ca simplu instrument de supraveghere. În plus, nu este necesară dezvoltarea unui nou cadru avansat de testare a rezilienței cibernetice, întrucât statele membre au adoptat deja la scară largă TIBER-UE, singurul astfel de cadru disponibil în UE în prezent.

4.3.4 Cerințele pentru verificatori nu ar trebui să fie incluse în corpul principal al regulamentului propus, întrucât sectorul legat de TLPT este încă în curs de dezvoltare, iar inovarea poate fi împiedicată prin impunerea unor cerințe specifice. Acestea fiind spuse, BCE este de părere că, pentru a asigura un grad ridicat de independență în efectuarea testelor, entitățile financiare nu ar trebui să angajeze sau să contracteze verificatori care sunt angajați sau contractați de entități financiare din propriul grup sau care sunt în alt mod deținuți și/sau controlați de entitățile financiare care urmează să fie testate.

4.3.5 Pentru a reduce riscul de fragmentare și a asigura armonizarea, regulamentul propus ar trebui să prevadă un cadru TLPT care să se aplice sectorului financiar din întreaga Uniune. Fragmentarea poate duce la creșterea costurilor și a cerințelor tehnice, operaționale, precum și a resurselor financiare, atât pentru autoritățile competente, cât și pentru instituțiile financiare. Aceste costuri și cerințe sporite pot avea, în cele din urmă, un impact negativ asupra recunoașterii reciproce a testelor. Această lipsă de armonizare și problemele rezultate în ceea ce privește recunoașterea reciprocă sunt deosebit de importante pentru entitățile financiare, care pot deține licențe multiple și/sau își pot desfășura activitatea în mai multe jurisdicții din întreaga Uniune. Standardele tehnice de reglementare și de punere în aplicare, care urmează să fie elaborate pentru TLPT în temeiul regulamentului propus, ar trebui să fie în conformitate cu TIBER-UE. De asemenea, BCE apreciază oportunitatea de a se implica în elaborarea acestor standarde tehnice de reglementare și de punere în aplicare în cooperare cu AES.

4.3.6 Implicarea activă a autorităților competente în testare ar putea duce la un potențial conflict de interese cu cealaltă funcție pe care o îndeplinesc, și anume evaluarea cadrului de testare al entității financiare. În acest context, BCE propune eliminarea din regulamentul propus a oricărei obligații a autorităților competente în ceea ce privește validarea documentelor și eliberarea unui atestat pentru un test TLPT.

4.4 Riscurile privind TIC generate de părți terțe

4.4.1 BCE consideră binevenită introducerea unui set cuprinzător de principii-cheie și a unui cadru solid de monitorizare pentru identificarea și gestionarea riscurilor privind TIC generate de furnizorii terți de servicii TIC, indiferent dacă aceștia aparțin aceluiași grup de entități financiare. Acestea fiind spuse, pentru a realiza o identificare și o gestionare eficace a riscurilor TIC, este important să se identifice și să se clasifice în mod corect, printre altele, furnizorii terți esențiali de servicii TIC. În acest sens, deși introducerea actelor delegate ([91]) care vor completa criteriile care urmează să fie utilizate în scopuri de clasificare ([92]) este binevenită, BCE ar trebui să fie consultată înainte de adoptarea unor astfel de acte delegate.

([89]) Disponibil pe website-ul BCE, la adresa www.ecb.europa.eu.
([90]) Articolele 23 și 24 din regulamentul propus.
([91]) A se vedea articolul 28 alineatul (3) din regulamentul propus.
([92]) A se vedea articolul 28 alineatul (2) din regulamentul propus.

4.4.2 În ceea ce privește structura cadrului de monitorizare ([93]), sunt necesare clarificări suplimentare cu privire la rolul care urmează să fie asumat de comitetul mixt. În același timp, BCE apreciază includerea sa în Forumul de monitorizare în calitate de observator, întrucât acest rol va oferi BCE același acces la documentație și informații ca și membrilor cu drept de vot ([94]). BCE ar dori să atragă atenția organelor legislative ale Uniunii asupra faptului că BCE, în calitatea sa de observator, ar contribui la activitatea Forumului de monitorizare, atât în calitatea sa de bancă centrală emitentă, responsabilă de monitorizarea infrastructurilor pieței, cât și în calitate de autoritate de supraveghere prudențială a instituțiilor de credit. În plus, BCE observă că, pe lângă faptul că va fi observator în cadrul Forumului de monitorizare, BCE va face parte, de asemenea, în calitate de autoritate competentă, din echipa comună de examinare. În acest sens, organele legislative ale Uniunii ar putea reflecta în continuare cu privire la componența echipelor comune de examinare ([95]), astfel încât să se asigure implicarea corespunzătoare a autorităților competente relevante. De asemenea, BCE consideră că numărul maxim de participanți la echipele comune de examinare ar trebui mărit, ținând seama de caracterul esențial, de complexitatea și de sfera serviciilor TIC furnizate de terți.

4.4.3 BCE constată că, în conformitate cu regulamentul propus, supervizorul principal poate împiedica furnizorului terț esențial de servicii TIC să încheie alte acorduri de subcontractare în cazul în care (i) subcontractantul avut în vedere este un furnizor terț de servicii TIC sau un subcontractant de servicii TIC stabilit într-o țară terță și (ii) subcontractarea vizează o funcție critică sau importantă a entității financiare. BCE dorește să sublinieze faptul că aceste competențe pot fi exercitate de supervizorul principal numai în contextul acordurilor de subcontractare în cazul în care un furnizor terț esențial de servicii TIC subcontractează o funcție critică sau importantă unei entități juridice separate stabilite într-o țară terță. BCE înțelege că supervizorul principal nu ar putea exercita competențe comparabile pentru a împiedica un furnizor terț esențial de servicii TIC să externalizeze funcțiile critice sau importante ale entității financiare către unitățile respectivului furnizor de servicii situate într-o țară terță. De exemplu, s-ar putea întâmpla ca, din punct de vedere operațional, datele și/sau informațiile esențiale să poată fi stocate sau prelucrate de unități situate în afara Spațiului Economic European (SEE). Într-un astfel de caz, este posibil ca supervizorul principal să nu acorde în mod adecvat autorităților competente acces la toate informațiile, sediile, infrastructurile și personalul relevant pentru îndeplinirea tuturor funcțiilor critice sau importante ale entității financiare. Pentru a se asigura că capacitatea autorităților competente de a-și îndeplini sarcinile în mod nestingherit, BCE sugerează că supervizorului principal ar trebui să i se acorde competența de a restricționa, de asemenea, utilizarea de către furnizorii terți esențiali de servicii TIC a unităților situate în afara SEE. Această competență ar putea fi exercitată în cazurile specifice în care nu există acorduri administrative cu autoritățile relevante din țările terțe, astfel cum se prevede în regulamentul propus ([96]), sau în care reprezentanții furnizorilor terți esențiali de servicii TIC nu oferă suficiente garanții în cadrul țării terțe relevante în ceea ce privește accesul la informații, sedii, infrastructură și personal, necesare pentru îndeplinirea sarcinilor de supraveghere sau de monitorizare.

4.4.4 În cele din urmă, a solicita autorităților competente să dea curs recomandărilor supervizorului principal ([97]) ar putea implica riscul ca acestea să se dovedească ineficace, întrucât este posibil ca autoritățile competente să nu aibă o viziune holistică asupra riscurilor generate de fiecare furnizor terț esențial de servicii TIC. În plus, autorităților competente li se poate solicita să ia măsuri împotriva entităților lor financiare supravegheate în cazul în care recomandările nu sunt aplicate de către furnizorii terți esențiali de servicii. În temeiul regulamentului propus ([98]), autoritățile competente pot solicita entităților lor financiare supravegheate să suspende temporar serviciul furnizat de furnizorul terț esențial sau să rezilieze contractele în derulare cu furnizorii terți esențiali de servicii. Este dificil ca procesul de monitorizare avut în vedere să fie transpus în acțiuni concrete. Mai precis, nu este clar dacă o entitate financiară supravegheată va fi în măsură să suspende sau să rezilieze un contract cu un furnizor terț esențial de servicii. Acest lucru se datorează faptului că furnizorul terț esențial de servicii TIC ar putea fi un furnizor semnificativ pentru entitatea financiară respectivă, ori costurilor și a daunelor, contractuale sau de altă natură, pe care entitatea financiară le poate suferi ca urmare a unei astfel de suspendări sau rezilieri. În plus, această abordare nu sprijină convergența monitorizării, deoarece autoritățile competente pot interpreta aceeași recomandare în mod divergent. Acest lucru ar putea împiedica, în cele din urmă, armonizarea avută în vedere și abordarea coerentă în ceea ce privește monitorizarea riscurilor generate de furnizori terți de servicii TIC la nivelul Uniunii. Având în vedere cele de mai sus, organele legislative ale Uniunii pot lua în considerare posibilitatea de a acorda supervizorilor legali competențe specifice de asigurare a respectării legislației în ceea ce privește furnizorii terți esențiali de servicii TIC, ținând seama de limitele impuse de jurisprudența Meroni, astfel cum a fost atenuată parțial de Curtea de Justiție în hotărârea sa în cauza ESMA ([99]).

([93]) A se vedea articolul 29 din regulamentul propus.
([94]) A se vedea articolul 29 alineatul (3) din regulamentul propus.
([95]) A se vedea articolul 35 din regulamentul propus.
([96]) A se vedea articolul 39 alineatul (1) din regulamentul propus.
([97]) A se vedea articolul 29 alineatul(4) și articolul 37 din regulamentul propus.
([98]) A se vedea articolul 37 alineatul (3) din regulamentul propus.
([99]) A se vedea Hotărârea Curții (Marea Cameră), 22 ianuarie 2014, Regatul Unit al Marii Britanii și Irlandei de Nord/Parlamentul European și Consiliul Uniunii Europene, Regulamentul (UE) 36/2012 — cauza C-270/12.

În cazul în care BCE recomandă modificarea regulamentului propus, propunerile de redactare specifice însoțite de o explicație în acest sens se regăsesc într-un document tehnic de lucru separat. Documentul tehnic de lucru este disponibil în limba engleză pe EUR-Lex.

Adoptat la Frankfurt pe Main, vineri, 4 iunie 2021.

Președinta BCE
Christine LAGARDE