I

(Rezoluții, recomandări și avize)

RECOMANDĂRI

COMITETUL EUROPEAN PENTRU RISC SISTEMIC

RECOMANDAREA COMITETULUI EUROPEAN PENTRU RISC SISTEMIC

din 2 decembrie 2021

privind un cadru paneuropean de coordonare sistemică a incidentelor cibernetice pentru autoritățile relevante

(CERS/2021/17)

(2022/C 134/01)

CONSILIUL GENERAL AL COMITETULUI EUROPEAN PENTRU RISC SISTEMIC,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Acordul privind Spațiul Economic European ([1]), în special anexa IX,

având în vedere Regulamentul (UE) nr. 1092/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 privind supravegherea macroprudențială la nivelul Uniunii Europene a sistemului financiar și de înființare a unui Comitet european pentru risc sistemic ([2]), în special articolul 3 alineatul (2) literele (b) și (d) și articolele 16 și 18,

având în vedere Decizia CERS/2011/1 a Comitetului european pentru risc sistemic din 20 ianuarie 2011 de adoptare a Regulamentului de procedură al Comitetului european pentru risc sistemic ([3]), în special articolele 18-20,

întrucât:

(1) Astfel cum se menționează în considerentul (4) al Recomandării CERS/2013/1 a Comitetului european pentru risc sistemic ([4]), obiectivul final al politicii macroprudențiale este de a contribui la salvgardarea stabilității sistemului financiar în ansamblu, inclusiv prin consolidarea rezilienței sistemului financiar și prin diminuarea acumulării de riscuri sistemice, asigurând pe această cale o contribuție sustenabilă a sectorului financiar la creșterea economică. Comitetul european pentru risc sistemic (CERS) răspunde de supravegherea macroprudențială a sistemului financiar în Uniune. În îndeplinirea mandatului său, CERS ar trebui să contribuie la prevenirea și atenuarea riscurilor sistemice la adresa stabilității financiare, inclusiv a celor legate de incidentele cibernetice, și să propună modalități de atenuare a acestor riscuri.

(2) Incidentele cibernetice majore pot prezenta un risc sistemic pentru sistemul financiar, având în vedere potențialul lor de a perturba serviciile și operațiunile financiare critice. Amplificarea unui șoc inițial poate avea loc fie prin contagiune operațională sau financiară, fie printr-o erodare a încrederii în sistemul financiar. Dacă sistemul financiar nu este în măsură să absoarbă aceste șocuri, stabilitatea financiară va fi în pericol, iar această situație poate duce la o criză cibernetică sistemică ([5]).

([1]) JO L 1, 3.1.1994, p. 3.
([2]) JO L 331, 15.12.2010, p. 1.
([3]) OJ C 58, 24.2.2011, p. 4.
([4]) Recomandarea CERS/2013/1 a Comitetului european pentru risc sistemic din 4 aprilie 2013 privind obiectivele intermediare și instrumentele politicii macroprudențiale (JO C 170, 15.6.2013, p. 1).
([5]) A se vedea „*Systemic cyber risk*" (Riscul cibernetic sistemic), CERS, februarie 2020, disponibil pe website-ul CERS la adresa www.esrb.europa.eu

(3) Evoluția constantă a sferei amenințărilor cibernetice și creșterea recentă a numărului incidentelor cibernetice majore sunt indicatori ai unui risc mai mare la adresa stabilității financiare în Uniune. Pandemia de COVID-19 a evidențiat importanța rolului pe care îl joacă tehnologia în facilitarea funcționării sistemului financiar. Autoritățile și instituțiile relevante au trebuit să își adapteze infrastructura tehnică și cadrele de gestionare a riscurilor la o creștere bruscă a lucrului la distanță, ceea ce a sporit expunerea generală a sistemului financiar la amenințările cibernetice și a permis infractorilor atât să conceapă noi moduri de operare, cât și să le adapteze pe cele existente pentru a exploata situația ([6]). În acest context, numărul incidentelor cibernetice raportate către Supravegherea Bancară a BCE în anul 2020 a crescut cu 54 % față de anul 2019 ([7]).

(4) Un eventual incident cibernetic major pe scară largă, cu viteză și rată de propagare sporite necesită un răspuns eficace din partea autorităților relevante pentru a atenua potențialele efecte negative asupra stabilității financiare. Coordonarea și comunicarea rapidă între autoritățile relevante la nivelul Uniunii pot contribui la evaluarea din timp a impactului unui incident cibernetic major asupra stabilității financiare, menținând încrederea în sistemul financiar și limitând contagiunea la alte instituții financiare, contribuind astfel la prevenirea transformării unui incident cibernetic major într-un risc la adresa stabilității financiare.

(5) Șocul subiacent are o origine inedită față de crizele financiare și de lichiditate tradiționale cu care se confruntă, de obicei, autoritățile relevante. Pe lângă aspectele financiare, evaluarea globală a riscurilor trebuie să includă amploarea și impactul perturbărilor operaționale, deoarece acestea ar putea influența alegerea instrumentelor macroprudențiale. În mod similar, stabilitatea financiară ar putea influența, de asemenea, alegerea de către experții cibernetici a factorilor operaționali de atenuare. Acest lucru necesită o coordonare strânsă și rapidă și o comunicare deschisă, pentru a putea, printre altele, consolida conștientizarea situației.

(6) Riscul unui eșec în coordonarea autorităților există și trebuie abordat. Autoritățile relevante din Uniune vor trebui să se coordoneze între ele și cu alte autorități, cum ar fi Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), cu care de obicei nu interacționează. Întrucât un număr semnificativ de instituții financiare din Uniune își desfășoară activitatea la nivel mondial, este posibil ca un incident cibernetic major să nu fie limitat la Uniune sau să fie declanșat din afara Uniunii și ar putea necesita coordonarea la nivel mondial a răspunsului.

(7) Autoritățile relevante trebuie să fie pregătite pentru aceste interacțiuni. În caz contrar, ar exista riscul ca acestea să ia măsuri inconsecvente care contrazic sau periclitează răspunsurile altor autorități. Un astfel de eșec în materie de coordonare ar putea amplifica șocul pentru sistemul financiar, ducând la o erodare a încrederii în funcționarea sistemului financiar care, în cel mai rău caz, ar reprezenta un risc pentru stabilitatea financiară ([8]). Prin urmare, ar trebui luate măsurile necesare pentru a aborda riscul la adresa stabilității financiare care decurge dintr-un eșec de coordonare în cazul unui incident cibernetic major.

(8) Raportul CERS (2021) „*Mitigating systemic cyber risk*" (Atenuarea riscului cibernetic sistemic) ([9]) identifică necesitatea de a institui un cadru paneuropean de coordonarea în cazul incidentelor cibernetice sistemice (EU-SCICF) pentru autoritățile relevante din Uniune. Obiectivul EU-SCICF ar fi acela de a crește nivelul de pregătire al autorităților relevante pentru a facilita un răspuns coordonat la un eventual incident cibernetic major. Raportul CERS (2021) „*Mitigating systemic cyber risk*" oferă evaluarea CERS cu privire la caracteristicile cadrului care ar fi necesare, *prima facie*, pentru a aborda riscul unui eșec de coordonare.

(9) Obiectivul principal al prezentei recomandări este de a valorifica unul dintre rolurile avute în vedere pentru autoritățile europene de supraveghere (AES) în propunerea de regulament al Parlamentului European și al Consiliului privind reziliența operațională digitală a sectorului financiar ([10]) (denumită în continuare „DORA") de a permite treptat un răspuns coordonat eficace la nivelul Uniunii în cazul unui incident transfrontalier major legat de tehnologiile informației și comunicațiilor (TIC) sau al unei amenințări conexe care ar avea un impact sistemic asupra sectorului financiar al Uniunii în ansamblu. Acest proces va conduce la crearea EU-SCICF pentru autoritățile relevante.

([6]) A se vedea „*Internet Organised Crime Threat Assessment*" (Evaluarea amenințării pe care o reprezintă criminalitatea organizată pe internet), Europol, 2020, disponibil pe website-ul Europol la adresa www.europol.europa.eu

([7]) A se vedea „*IT and cyber risk: a constant challenge*" (Tehnologia informației și riscul cibernetic: o provocare constantă), BCE, 2021, disponibil pe website-ul privind supravegherea bancară al BCE, la adresa www.bankingsupervision.europa.eu

([8]) A se vedea „Systemic cyber risk" (Riscul cibernetic sistemic), CERS, februarie 2020, disponibil pe website-ul CERS la adresa www.esrb.europa.eu

([9]) A se vedea „Mitigating systemic cyber risk" (Atenuarea riscului cibernetic sistemic), CERS, 2021, (publicat ulterior).

([10]) COM(2020) 595 final.

(10) EU-SCICF nu ar trebui să vizeze înlocuirea cadrelor existente, ci eliminarea oricăror lacune în materie de coordonare și comunicare între autoritățile relevante, precum și cu alte autorități din Uniune și cu alți actori-cheie la nivel internațional. În acest sens, ar trebui luată în considerare poziționarea EU-SCICF în actualul cadru referitor la criza financiară și în cel al Uniunii în materie de incidente cibernetice. În ceea ce privește coordonarea între autoritățile relevante în sine, ar trebui să se ia în considerare, fără a se limita la acestea, rolurile și activitățile Grupului de cooperare pentru rețele și sisteme informatice (NIS) pentru entitățile financiare prevăzute de Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului ([11]) și mecanismele de coordonare avute în vedere prin instituirea unității cibernetice comune, alături de implicarea ENISA.

(11) În special, propunerea de a lansa pregătirea EU-SCICF urmărește să aprobe rolurile potențiale ale AES, astfel cum sunt prevăzute în propunerea DORA. DORA propune ca „AES, prin intermediul Comitetului comun și în colaborare cu autoritățile competente, Banca Centrală Europeană (BCE) și CERS, să poată stabili mecanisme care să permită schimbul de practici eficace între sectoarele financiare în vederea îmbunătățirii conștientizării situației și a identificării vulnerabilităților și riscurilor cibernetice comune la nivelul tuturor sectoarelor” și „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” ([12]). Un cadru paneuropean, cum ar fi EU-SCICF, nu există încă și ar trebui instituit și dezvoltat în contextul DORA.

(12) Având în vedere riscul la adresa stabilității financiare din Uniune care decurge din riscul cibernetic, lucrările pregătitoare pentru instituirea treptată a EU-SCICF ar trebui, în măsura posibilului, să înceapă chiar înainte de a fi pe deplin aplicabil cadrul juridic și de politică necesar pentru instituirea sa. Acest cadru juridic și de politică va fi complet finalizat odată ce dispozițiile relevante ale DORA și ale actelor sale delegate vor deveni aplicabile.

(13) O comunicare eficace contribuie la conștientizarea situației în rândul autorităților relevante și, prin urmare, este o condiție prealabilă indispensabilă pentru coordonarea la nivelul Uniunii în timpul incidentelor cibernetice majore. În acest sens, ar trebui definită infrastructura de comunicații necesară pentru coordonarea răspunsului la un incident cibernetic major. Acest lucru ar implica precizarea tipului de informații care trebuie partajate, a canalelor regulate care trebuie utilizate pentru schimbul de astfel de informații și a punctelor de contact cu care ar trebui să se facă schimb de informații. Schimbul de informații trebuie să respecte cerințele legale existente. În plus, ar putea fi necesar ca autoritățile relevante să definească un plan de acțiune clar și protocoalele care trebuie respectate pentru a asigura o coordonare adecvată între autoritățile implicate în planificarea unui răspuns coordonat la un incident cibernetic major.

(14) O criză cibernetică sistemică va necesita instituirea unei cooperări depline la nivel național și la nivelul Uniunii. Prin urmare, se poate avea în vedere desemnarea unor puncte de contact pentru AES, BCE și fiecare stat membru dintre autoritățile sale naționale relevante, care ar trebui să fie comunicate AES, pentru a stabili principalii interlocutori ai sistemului de coordonare al EU-SCICF care să fie informați în cazul unui incident cibernetic major. Necesitatea de a desemna puncte de contact ar trebui evaluată în cursul dezvoltării EU-SCICF, ținând seama de punctul unic de contact desemnat în temeiul Directivei (UE) 2016/1148 pe care statele membre l-au stabilit cu privire la securitatea rețelelor și a sistemelor informatice pentru a asigura cooperarea transfrontalieră cu alte state membre și cu Grupul de cooperare NIS ([13]).

(15) Desfășurarea de exerciții de gestionare a crizelor și de intervenție în situații de urgență ar putea facilita punerea în aplicare a EU-SCICF și ar permite autorităților să evalueze gradul lor de pregătire pentru o criză cibernetică sistemică la nivelul Uniunii. Astfel de exerciții ar permite autorităților să tragă niște concluzii și ar permite îmbunătățirea și evoluția continuă a EU-SCICF.

([11]) 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).

([12]) A se vedea proiectul de articol 43 din propunerea pentru DORA.

([13]) A se vedea Comisia Europeană, Grupul de cooperare NIS, disponibil pe website-ul Comisiei Europene, la adresa www.ec.europa.eu

(16) Pentru dezvoltarea EU-SCICF, este esențial ca AES să desfășoare împreună activități pregătitoare relevante pentru a lua în considerare potențialele elemente-cheie ale cadrului, precum și resursele și nevoile necesare pentru a continua dezvoltarea acestuia. Ulterior, AES ar putea începe să lucreze la o analiză preliminară a oricăror obstacole care ar putea afecta capacitatea AES și a autorităților relevante de a înființa EU-SCICF și de a face schimb de informații relevante prin intermediul canalelor de comunicare în cazul unui incident cibernetic major. O astfel de analiză ar constitui un pas important care ar sta la baza oricărei acțiuni ulterioare, fie de natură legislativă fie a altor inițiative de sprijin pe care Comisia Europeană le-ar putea lua în etapa de punere în aplicare post-DORA,

ADOPTĂ PREZENTA RECOMANDARE:

SECȚIUNEA 1

RECOMANDĂRI

Recomandarea A – Instituirea unui cadru paneuropean de coordonare a incidentelor cibernetice sistemice (EU-SCICF)

1. Se recomandă ca, astfel cum se prevede în propunerea Comisiei de regulament al Parlamentului European și al Consiliului privind reziliența operațională digitală a sectorului financiar (denumită în continuare „DORA”), autoritățile europene de supraveghere (AES), în solidar prin Comitetul comun și împreună cu Banca Centrală Europeană (BCE), Comitetul european pentru risc sistemic (CERS) și autoritățile naționale relevante, să înceapă pregătirile pentru dezvoltarea treptată a unui răspuns coordonat eficace la nivelul Uniunii în cazul unui incident cibernetic transfrontalier major sau al unei amenințări conexe care ar putea avea un impact sistemic asupra sectorului financiar al Uniunii. Lucrările pregătitoare în vederea unui răspuns coordonat la nivelul Uniunii ar trebui să implice dezvoltarea treptată a EU-SCICF pentru AES, BCE, CERS și autoritățile naționale relevante. Aceasta ar trebui să includă, de asemenea, o evaluare a necesarului de resurse pentru dezvoltarea eficace a EU-SCICF.

2. Se recomandă ca AES să efectueze, având în vedere subrecomandarea A(1), în consultare cu BCE și CERS, o cartografiere și o analiză ulterioară a obstacolelor actuale, a obstacolelor juridice și a altor obstacole operaționale din calea dezvoltării eficiente a EU-SCICF.

Recomandarea B – Stabilirea punctelor de contact ale EU-SCICF

Se recomandă desemnarea de către AES, BCE și fiecare stat membru, din rândul autorităților lor naționale relevante, a unui punct principal de contact care ar trebui comunicat AES. Această listă de contacte va facilita dezvoltarea cadrului și, odată ce EU-SCICF va fi instituit, punctele de contact și CERS ar trebui să fie informate în cazul unui incident cibernetic major. De asemenea, ar trebui avută în vedere coordonarea între EU-SCICF și punctul unic de contact desemnat în temeiul Directivei (UE) 2016/1148 pe care statele membre l-au instituit cu privire la securitatea rețelelor și a sistemelor informatice pentru a asigura cooperarea transfrontalieră cu alte state membre și cu Grupul de cooperare pentru rețele și sisteme informatice.

Recomandarea C – Măsuri adecvate la nivelul Uniunii

Se recomandă ca, pe baza rezultatelor analizelor efectuate în conformitate cu recomandarea A, Comisia să ia în considerare măsurile adecvate necesare pentru a asigura coordonarea eficace a răspunsurilor la incidentele cibernetice sistemice.

SECȚIUNEA 2

PUNERE ÎN APLICARE

1. **Definiții**

În sensul prezentei recomandări, se aplică următoarele definiții:

(a) „cibernetic” înseamnă legat de, din cadrul sau prin intermediul infrastructurii informaționale interconectate a interacțiunilor dintre persoane, procese, date și sisteme de informații ([14]);

([14]) A se vedea Cyber Lexicon, FSB, 12 noiembrie 2018, disponibil pe website-ul FSB la adresa www.fsb.org.

(b) „incident cibernetic major” înseamnă un incident legat de TIC cu un potențial impact negativ major asupra rețelelor și a sistemelor informatice care sprijină funcțiile critice ale entităților financiare ([15]);

(c) „criză cibernetică sistemică” înseamnă un incident cibernetic major care provoacă un nivel de perturbare a sistemului financiar al Uniunii care ar putea avea consecințe negative grave pentru buna funcționare a pieței interne și pentru funcționarea economiei reale. O astfel de criză ar putea rezulta dintr-un incident cibernetic major care cauzează șocuri pe o serie de canale, inclusiv operaționale, de încredere și financiare;

(d) „autorități europene de supraveghere” sau „AES” înseamnă Autoritatea europeană de supraveghere (Autoritatea bancară europeană), instituită prin Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului ([16]), împreună cu Autoritatea europeană de supraveghere (Autoritatea europeană pentru asigurări și pensii ocupaționale), instituită prin Regulamentul (UE) nr. 1094/2010 al Parlamentului European și al Consiliului ([17]) și Autoritatea europeană de supraveghere (Autoritatea europeană pentru valori mobiliare și piețe) instituită prin Regulamentul (UE) nr. 1095/2010 al Parlamentului European și al Consiliului (denumite, în continuare, în mod colectiv „AES”) ([18]).

(e) „comitet comun” înseamnă Comitetul comun al autorităților europene de supraveghere prevăzut la articolul 54 din Regulamentul (UE) nr. 1093/2010, Regulamentul (UE) nr. 1094/2010 și Regulamentul (UE) nr. 1095/2010;

(f) „autoritate națională relevantă” înseamnă

1. o autoritate competentă sau de supraveghere dintr-un stat membru, astfel cum se specifică în actele Uniunii menționate la articolul 1 alineatul (2) din Regulamentul (UE) nr. 1093/2010, din Regulamentul (UE) nr. 1094/2010 și din Regulamentul (UE) nr. 1095/2010, precum și orice altă autoritate națională competentă, astfel cum se specifică în actele Uniunii care conferă sarcini AES;

2. o autoritate competentă dintr-un stat membru desemnată în conformitate cu:

i. articolul 4 din Directiva 2013/36/UE a Parlamentului European și a Consiliului ([19]), fără a aduce atingere atribuțiilor specifice conferite BCE prin Regulamentul (UE) nr. 1024/2013 al Consiliului ([20]);

ii. articolul 22 din Directiva (UE) 2015/2366 a Parlamentului European și a Consiliului ([21]);

iii. articolul 37 din Directiva 2009/110/CE a Parlamentului European și a Consiliului ([22]);

iv. articolul 4 din Directiva (UE) 2019/2034 a Parlamentului European și a Consiliului ([23]);

([15]) A se vedea articolul 3 punctul 7 din DORA .

([16]) 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).

([17]) 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).

([18]) 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).

([19]) 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).

([20]) 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).

([21]) 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).

([22]) 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).

([23]) 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).

v. articolul 3 alineatul (1) litera (ee) prima liniuță din propunerea de regulament al Parlamentului European și al Consiliului privind piețele criptoactivelor și de modificare a Directivei (UE) 2019/1937 ([24]);

vi. articolul 11 din Regulamentul (UE) nr. 909/2014 al Parlamentului European și al Consiliului ([25]);

vii. articolul 22 din Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului ([26]);

viii. articolul 67 din Directiva 2014/65/UE a Parlamentului European și a Consiliului ([27]),

ix. articolul 22 din Regulamentul (UE) nr. 648/2012;

x. articolul 44 din Directiva 2011/61/UE a Parlamentului European și a Consiliului ([28]),

xi. articolul 97 din Directiva 2009/65/CE a Parlamentului European și a Consiliului ([29]);

xii. articolul 30 din Directiva 2009/138/CE a Parlamentului European și a Consiliului ([30]);

xiii. articolul 12 din Directiva (UE) 2016/97 a Parlamentului European și a Consiliului ([31]);

xiv. articolul 47 din Directiva (UE) 2016/2341 a Parlamentului European și a Consiliului ([32]);

xv. articolul 22 din Regulamentul (CE) nr. 1060/2009 al Parlamentului European și al Consiliului ([33]);

xvi. articolul 3 alineatul (2) și articolul 32 din Directiva 2006/43/CE a Parlamentului European și a Consiliului ([34]);

xvii. articolul 40 din Regulamentul (UE) nr. 2016/1011 al Parlamentului European și al Consiliului ([35]);

xviii. articolul 29 din Regulamentul (UE) nr. 2020/1503 al Parlamentului European și al Consiliului ([36]);

([24]) COM(2020) 593 final.

([25]) 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).

([26]) 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).

([27]) 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).

([28]) 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) 1095/2010 (JO L 174, 1.7.2011, p. 1).

([29]) 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).

([30]) 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).

([31]) 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).

([32]) 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).

([33]) 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)

([34]) Directiva 2006/43/CE a Parlamentului European 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).

([35]) 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).

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

3. o autoritate însărcinată cu adoptarea și/sau activarea măsurilor de politică macroprudențială sau cu alte atribuții de stabilitate financiară, cum ar fi analiza justificativă aferentă, inclusiv, dar fără a se limita la:

   i. o autoritate desemnată în temeiul titlului VII capitolul 4 din Directiva 2013/36/UE sau al articolul 458 alineatul (1) din Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului ([37]);

   ii. autoritatea macroprudențială care are obiectivele, mecanismele, atribuțiile, competențele, instrumentele și cerințele privind asumarea răspunderii, precum și alte caracteristici stabilite în Recomandarea CERS/2011/3 a Comitetului european pentru risc sistemic ([38]);

(g) „autoritate relevantă" înseamnă

1. o AES;

2. BCE pentru atribuțiile care îi sunt conferite în conformitate cu articolul 4 alineatele (1) și (2) și cu articolul 5 alineatul (2) din Regulamentul (UE) nr. 1024/2013;

3. o autoritate națională relevantă.

2. **Criterii de punere în aplicare**

Aplicarea prezentei recomandări trebuie să țină cont de următoarele criterii:

(a) principiul proporționalității și cel al necesității de a cunoaște ar trebui respectate în mod corespunzător, ținându-se totodată cont de obiectivul și cuprinsul fiecărei recomandări;

(b) ar trebui îndeplinite criteriile specifice de conformitate stabilite în anexă în legătură cu fiecare recomandare.

3. **Calendar pentru măsurile aplicate ca urmare a recomandării**

În conformitate cu articolul 17 alineatul (1) din Regulamentul (UE) nr. 1092/2010, destinatarii trebuie să comunice Parlamentului European, Consiliului, Comisiei și CERS acțiunile întreprinse drept răspuns la prezenta recomandare sau să justifice orice lipsă de acțiune. Destinatarii trebuie să transmită o astfel de comunicare în conformitate cu următoarele termene:

1. Recomandarea A

(a) Până la 30 iunie 2023, dar nu mai devreme de șase luni de la intrarea în vigoare a DORA, AES sunt invitate să transmită Parlamentului European, Consiliului, Comisiei și CERS un raport intermediar privind punerea în aplicare a subrecomandării A(1).

(b) Până la 30 iunie 2024, dar nu mai devreme de 18 luni de la intrarea în vigoare a DORA, AES sunt invitate să transmită Parlamentului European, Consiliului, Comisiei și CERS un raport final privind punerea în aplicare a subrecomandării A(1).

(c) Până la 30 iunie 2025, dar nu mai devreme de 30 luni de la intrarea în vigoare a DORA, AES sunt invitate să transmită Parlamentului European, Consiliului, Comisiei și CERS un raport privind punerea în aplicare a subrecomandării A(2).

2. Recomandarea B

Până la 30 iunie 2023, dar nu mai devreme de șase luni de la intrarea în vigoare a DORA, AES, BCE și statele membre sunt invitate să transmită Parlamentului European, Consiliului, Comisiei și CERS un raport privind punerea în aplicare a Recomandării B.

3. Recomandarea C

(a) Până la 31 decembrie 2023, dar nu mai devreme de 12 luni de la intrarea în vigoare a DORA, Comisia este invitată să prezinte Parlamentului European, Consiliului și CERS un raport privind punerea în aplicare a Recomandării C în vederea raportului intermediar al AES în conformitate cu subrecomandarea A(1).

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

([38]) Recomandarea CERS/2011/3 a Comitetului european pentru risc sistemic din 22 decembrie 2011 privind mandatul macroprudențial al autorităților naționale (JO C 41, 14.2.2012, p. 1).

(b) Până la 31 decembrie 2025, dar nu mai devreme de 36 luni de la intrarea în vigoare a DORA, Comisia este invitată să transmită Parlamentului European, Consiliului și CERS un raport privind punerea în aplicare a Recomandării C în vederea rapoartelor AES în conformitate cu recomandarea A.

4. **Monitorizare și evaluare**

1. Secretariatul CERS:

(a) va oferi asistență destinatarilor, asigurând coordonarea raportării și furnizarea de modele relevante și, dacă este cazul, informații detaliate privind procedura și calendarul pentru măsurile adoptate în urma recomandării;

(b) va verifica măsurile aplicate de destinatari, va acorda asistență la cerere și va prezenta Consiliului general rapoarte privind măsurile aplicate. Evaluările vor fi inițiate după cum urmează:

(i) în termen de 12 luni de la intrarea în vigoare a DORA, în ceea ce privește punerea în aplicare a recomandărilor A și B;

(ii) în termen de 18 luni de la intrarea în vigoare a DORA, în ceea ce privește punerea în aplicare a Recomandării C;

(iii) în termen de 24 luni de la intrarea în vigoare a DORA, în ceea ce privește punerea în aplicare a Recomandării A;

(iv) în termen de 36 luni de la intrarea în vigoare a DORA, în ceea ce privește punerea în aplicare a Recomandării A;

(v) în termen de 42 luni de la intrarea în vigoare a DORA, în ceea ce privește punerea în aplicare a Recomandării C;

2. Consiliul general va evalua măsurile și justificările raportate de către destinatari și, după caz, va putea decide că prezenta recomandare nu a fost respectată și destinatarul nu a justificat în mod adecvat lipsa de acțiune.

Adoptată la Frankfurt pe Main, joi, 2 decembrie 2021..

Șeful secretariatului CERS,
în numele Consiliului general al CERS
Francesco MAZZAFERRO

ANEXĂ

PRECIZAREA CRITERIILOR DE CONFORMITATE APLICABILE RECOMANDĂRILOR

Recomandarea A – Instituirea unui cadru paneuropean de coordonare a incidentelor cibernetice sistemice (EU-SCICF)

Pentru **subrecomandarea A(1),** se prevăd următoarele criterii de conformitate.

1. Atunci când se pregătește un răspuns coordonat eficace la nivelul Uniunii, care ar trebui să implice dezvoltarea treptată a EU-SCICF prin exercitarea competenței prevăzute în viitorul Regulament al Parlamentului European și al Consiliului privind reziliența operațională digitală a sectorului financiar (denumit în continuare „DORA”), autoritățile europene de supraveghere (AES), acționând prin intermediul Comitetului comun și împreună cu Banca Centrală Europeană (BCE), Comitetul european pentru risc sistemic (CERS) și autoritățile naționale relevante, și în consultare cu Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor și cu Comisia, atunci când se consideră necesar, ar trebui să ia în considerare includerea în pregătirea preconizată pentru EU-SCICF a cel puțin următoarelor aspecte:

   a. analiza necesarului de resurse pentru dezvoltarea eficientă a EU-SCICF;

   b. dezvoltarea unor exerciții de gestionare a crizelor și de intervenție în situații de urgență care implică scenarii de atac cibernetic, în vederea dezvoltării canalelor de comunicare;

   c. dezvoltarea unui vocabular comun;

   d. dezvoltarea unei clasificări coerente a incidentelor cibernetice;

   e. instituirea unor canale sigure și fiabile de schimb de informații, inclusiv a unor sisteme de rezervă;

   f. stabilirea de puncte de contact;

   g. abordarea confidențialității în ceea ce privește schimbul de informații;

   h. colaborarea și inițiativele de schimb de informații cu serviciile de informații cibernetice din sectorul financiar;

   i. dezvoltarea unor procese eficace de activare și escaladare prin conștientizarea situației;

   j. clarificarea responsabilităților participanților la cadru;

   k. dezvoltarea de interfețe pentru coordonarea transsectorială și, după caz, a țărilor terțe;

   l. asigurarea unei comunicări coerente între autoritățile relevante și public, pentru a păstra încrederea;

   m. stabilirea unor linii de comunicare predefinite pentru comunicarea în timp util;

   n. efectuarea unor exerciții adecvate de testare a cadrului, inclusiv teste interjurisdicționale și coordonarea țărilor terțe, precum și evaluări care au ca rezultat lecțiile învățate și evoluția cadrului;

   o. asigurarea unei comunicări eficace și a unor contramăsuri împotriva dezinformării.

Recomandarea B – Stabilirea punctelor de contact ale EU-SCICF

Pentru **Recomandarea B,** se prevăd următoarele criterii de conformitate.

1. AES, BCE și fiecare stat membru, prin autoritățile lor naționale relevante, ar trebui să convină asupra unei abordări comune privind partajarea și actualizarea listei punctelor de contact desemnate ale EU-SCICF.

2. Desemnarea punctului de contact ar trebui să fie evaluată ținând seama de punctul unic de contact desemnat în temeiul Directiva (UE) 2016/1148 pe care statele membre l-au instituit în ceea ce privește securitatea rețelelor și a sistemelor informatice pentru a asigura cooperarea transfrontalieră cu alte state membre și cu Grupul de cooperare pentru rețele și sisteme informatice.

Recomandarea C — Modificarea cadrului juridic al Uniunii

Pentru **Recomandarea C,** se stabilește următorul criteriu de conformitate.

Comisia ar trebui să analizeze dacă sunt necesare măsuri, inclusiv modificări ale legislației relevante a Uniunii, ca urmare a analizei efectuate în conformitate cu Recomandarea A, pentru a se asigura că AES, prin intermediul Comitetului comun și împreună cu BCE, CERS și autoritățile naționale relevante, pot dezvolta EU-SCICF în conformitate cu subrecomandarea A(1) și pentru a se asigura că AES, BCE, CERS și autoritățile naționale relevante, precum și alte autorități se pot implica în acțiuni de coordonare și schimburi de informații suficient de detaliate și de consecvente pentru a sprijini un EU-SCICF eficace.