I.

(Rezolucije, preporuke i mišljenja)

PREPORUKE

EUROPSKI ODBOR ZA SISTEMSKE RIZIKE

PREPORUKA EUROPSKOG ODBORA ZA SISTEMSKE RIZIKE

od 2. prosinca 2021.

o paneuropskom okviru za sistemsku koordinaciju kiberincidenata za relevantna tijela

(ESRB/2021/17)

(2022/C 134/01)

OPĆI ODBOR EUROPSKOG ODBORA ZA SISTEMSKE RIZIKE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Sporazum o Europskom gospodarskom prostoru ([1]), a posebno njegov Prilog IX.,

uzimajući u obzir Uredbu (EU) br. 1092/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o makrobonitetnom nadzoru financijskog sustava Europske unije i osnivanju Europskog odbora za sistemske rizike ([2]), a osobito njezin članak 3. stavak 2. točke (b), i (d) te članke 16. i 18.,

uzimajući u obzir Odluku ESRB/2011/1 Europskog odbora za sistemske rizike od 20. siječnja 2011. o donošenju Poslovnika Europskog odbora za sistemske rizike ([3]), a osobito njezine članke od 18. do 20.,

budući da:

(1) Kako je navedeno u uvodnoj izjavi 4. Preporuke ESRB/2013/1 Europskog odbora za sistemske rizike ([4]), krajnji cilj makrobonitetne politike je doprinijeti zaštiti stabilnosti financijskog sustava kao cjeline, uključujući jačanje otpornosti financijskog sustava i smanjenje stvaranja sistemskih rizika osiguravajući na taj način održiv doprinos financijskog sektora ekonomskom rastu. Europski odbor za sistemske rizike (ESRB) odgovoran je za makrobonitetni nadzor financijskog sustava unutar Unije. Pri ispunjavanju svojih ovlasti ESRB bi trebao doprinijeti sprečavanju i ublažavanju sistemskih rizika za financijsku stabilnost, uključujući one povezane s kiberincidentima, te predložiti kako bi se ti rizici mogli ublažiti.

(2) Veliki kiberincidenti mogu predstavljati sistemski rizik za financijski sustav s obzirom na njihov potencijal za ometanje ključnih financijskih usluga i operacija. Do povećanja početnog šoka može doći ili zbog operativne ili financijske zaraze ili slabljenja povjerenja u financijski sustav. Ako financijski sustav ne može apsorbirati te šokove, financijska stabilnost bit će ugrožena i ta situacija može dovesti do sustavne kiberkrize ([5]).

([1]) SL L 1, 3.1. 1994., str. 3.
([2]) SL L 331, 15.12. 2010., str. 1.
([3]) SL C 58, 24.2.2011., str. 4.
([4]) Preporuka ESRB/2013/1 Europskog odbora za sistemske rizike od 4. travnja 2013. o privremenim ciljevima i instrumentima makrobonitetne politike (SL C 170, 15.6.2013., str. 1.).
([5]) Vidi Systemic cyber risk (Sistemski kiberrizik), ESRB, veljača 2020., dostupno na internetskoj stranici ESRB-a na www.esrb.europa.eu

(3) Okruženje kiberprijetnji koje se neprestano razvija i nedavno povećanje velikih kiberincidenata pokazatelji su većeg rizika za financijsku stabilnost Unije. Pandemija bolesti COVID-19 istaknula je važnost uloge koju tehnologija ima u omogućivanju funkcioniranja financijskog sustava. Relevantna tijela i institucije trebali su prilagoditi svoju tehničku infrastrukturu i okvire za upravljanje rizicima iznenadnom povećanju rada na daljinu, što je povećalo ukupnu izloženost financijskog sustava kiberprijetnjama i omogućilo kriminalcima da osmisle nove načine rada i prilagode postojeće kako bi iskoristili situaciju ([6]). U tom se kontekstu broj kiberincidenata prijavljenih nadzoru banaka ESB-a 2020. povećao za 54 % u odnosu na 2019 ([7]).

(4) Potencijalno veliki razmjeri, brzina i stopa širenja velikog kibernetičkog incidenta zahtijevaju učinkovit odgovor relevantnih tijela kako bi se ublažili mogući negativni učinci na financijsku stabilnost. Brza koordinacija i komunikacija među relevantnim tijelima na razini Unije može pomoći u ranoj procjeni učinka velikog kiberincidenata na financijsku stabilnost, održavanje povjerenja u financijski sustav i ograničavanje širenja na druge financijske institucije te tako pridonijeti sprečavanju da veliki kiberincident postane rizik za financijsku stabilnost.

(5) Temeljni šok nastaje na nov način u usporedbi s tradicionalnom financijskom krizom i krizom likvidnosti s kojom se obično suočavaju relevantna tijela. Osim financijskih aspekata, ukupna procjena rizika mora uključivati opseg i učinak operativnih poremećaja jer bi oni mogli utjecati na odabir makrobonitetnih alata. Isto tako, financijska stabilnost bi mogla utjecati i na izbor operativnih mogućnosti ublažavanja od strane stručnjaka za kibersigurnost. To zahtijeva blisku i brzu koordinaciju i otvorenu komunikaciju kako bi se, među ostalim, izgradila informiranost o stanju.

(6) Rizik neuspjeha u koordinaciji između tijela postoji i potrebno ga je riješiti. Relevantna tijela u Uniji morat će se koordinirati međusobno i s drugim tijelima, kao što je Agencija Europske unije za kibersigurnost (ENISA), s kojom obično nisu u komunikaciji. Budući da znatan broj financijskih institucija Unije djeluje na globalnoj razini, veliki kiberincident vjerojatno neće biti ograničen na Uniju ili bi mogao nastati izvan Unije te bi mogao zahtijevati koordinaciju globalnog odgovora.

(7) Relevantna tijela moraju biti pripremljena za te interakcije. U protivnom bi mogli poduzeti nedosljedne mjere koje su u suprotnosti s odgovorima drugih tijela ili ih ugrožavaju. Takav neuspjeh koordinacije mogao bi pojačati šok za financijski sustav jer bi doveo do narušavanja povjerenja u funkcioniranje financijskog sustava, što bi u najgorem slučaju predstavljalo rizik za financijsku stabilnost ([8]). Stoga bi trebalo poduzeti potrebne korake za rješavanje rizika za financijsku stabilnost koji proizlazi iz neuspjeha koordinacije u slučaju velikog kiberincidenta.

(8) U izvješću ESRB-a (2021.) „*Ublažavanje sistemskog kiberrizika*" ([9]) utvrđena je potreba za uspostavom paneuropskog okvira za koordinaciju sistemskih kiberincidenata (EU-SCICF) za relevantna tijela u Uniji. Cilj EU-SCICF-a bio bi povećati razinu pripravnosti relevantnih tijela kako bi se olakšao koordinirani odgovor na potencijalno veliki kiberincident. U izvješću ESRB-a (2021.) „*Ublažavanje sistemskog kiberrizika*" daje se ESRB-ova procjena značajki okvira koje bi bile potrebne, prima facie, kako bi se uklonio rizik od neuspjeha koordinacije.

(9) Ključni je cilj ove Preporuke nadovezati se na jednu od predviđenih uloga europskih nadzornih tijela u okviru Prijedloga uredbe Europskog parlamenta i Vijeća o digitalnoj operativnoj otpornosti za financijski sektor ([10]) (u daljnjem tekstu „DORA") postupnog omogućivanja učinkovitog koordiniranog odgovora na razini Unije u slučaju velikog prekograničnog incidenta povezanog s informacijskim i komunikacijskim tehnologijama (IKT) ili povezane prijetnje sa sustavnim učinkom na financijski sektor Unije u cjelini. Taj će postupak dovesti do stvaranja EU-SCICF-a za relevantna tijela.

([6]) Vidi Internet Organised Crime Threat Assessment (Procjena prijetnje organiziranog kriminala na internetu), Europol, 2020., dostupno na mrežnim stranicama Europola na www.europol.europa.eu

([7]) Vidi IT and cyber risk: a constant challenge (Informatički i kiberrizik: stalni izazov, ESB, 2021., dostupno na mrežnim stranicama nadzora banaka ESB-a www.bankingsupervision.europa.eu.

([8]) Vidi Systemic cyber risk (Sistemski kiberrizik), ESRB, veljača 2020., dostupno na mrežnoj stranici ESRB-a na www.esrb.europa.eu

([9]) Vidi Ublažavanje sistemskog kiberrizika, ESRB,2021., (predstojeći).

([10]) COM (2020) 595 konačno.

(10) Cilj EU-SCICF-a ne bi trebao biti zamjena postojećih okvira, već premošćivanje praznina u koordinaciji i komunikaciji između samih relevantnih tijela i s drugim tijelima u Uniji i drugim ključnim akterima na međunarodnoj razini. U tom bi pogledu trebalo razmotriti pozicioniranje EU-SCICF-a u postojeći okviru za upravljanje financijskom krizom i okvir Unije za kiberincidente. Kad je riječ o koordinaciji među samim relevantnim tijelima, trebalo bi razmotriti, među ostalim, uloge i aktivnosti Skupine za suradnju u području mrežnih i informacijskih sustava (NIS) za financijske subjekte u skladu s Direktivom (EU) 2016/1148 Europskog parlamenta i Vijeća ([11]) te koordinacijske mehanizme predviđene osnivanjem Zajedničke jedinice za kibersigurnost uz sudjelovanje ENISA-e.

(11) Konkretno, cilj je prijedloga za pokretanje pripreme EU-SCICF-a podržati potencijalne uloge europskih nadzornih tijela, kako je predviđeno prijedlogom DORA-e. DORA predlaže da „europska nadzorna tijela, putem Zajedničkog odbora i u suradnji s nadležnim tijelima, Europskom središnjom bankom (ESB) i ESRB-om, mogu uspostaviti mehanizme kojima bi se omogućila razmjena učinkovitih praksi među financijskim sektorima radi poboljšanja informiranosti o stanju i utvrđivanja zajedničkih međusektorskih slabih točki u pogledu kibersigurnosti i rizika” i „mogu razviti vježbe za upravljanje krizom i izvanrednim situacijama koje uključuju scenarije kibernapada u cilju razvoja komunikacijskih kanala i postupnog omogućavanja učinkovitog koordiniranog odgovora na razini EU-a u slučaju velikog prekograničnog IKT incidenta ili povezane prijetnje sa sustavnim učinkom na financijski sektor Unije u cjelini” ([12]). Paneuropski okvir kao što je EU-SCICF još ne postoji te bi ga trebalo uspostaviti i razviti u kontekstu DORA-e.

(12) S obzirom na rizik za financijsku stabilnost Unije koji proizlazi iz kiberrizika, pripremni rad za postupnu uspostavu EU-SCICF-a trebao bi, u mjeri u kojoj je to izvedivo, započeti čak i prije nego što se u potpunosti počne primjenjivati potreban pravni i politički okvir za njegovu uspostavu. Taj bi pravni i politički okvir bio u potpunosti dovršen i finaliziran nakon što relevantne odredbe DORA-e i njezinih delegiranih akata postanu primjenjive.

(13) Učinkovita komunikacija doprinosi informiranosti o stanju među relevantnim tijelima te je stoga neophodan preduvjet za koordinaciju na razini Unije tijekom velikih kiberincidenata. U tom bi pogledu trebalo definirati komunikacijsku infrastrukturu potrebnu za koordinaciju odgovora na veliki kiberincident. To bi podrazumijevalo utvrđivanje vrste informacija koje je potrebno razmjenjivati, redovitih kanala koji će se upotrebljavati za razmjenu takvih informacija i kontaktnih točaka s kojima bi se informacije trebale razmjenjivati. Razmjena informacija mora biti u skladu s postojećim pravnim zahtjevima. Osim toga, relevantna tijela možda će morati utvrditi jasan akcijski plan i protokole koje treba slijediti kako bi se osigurala odgovarajuća koordinacija među tijelima uključenima u planiranje koordiniranog odgovora na veliki kiberincident.

(14) Sustavna kiberkriza zahtijevat će uspostavu potpune suradnje na nacionalnoj razini i razini Unije. Stoga se može predvidjeti određivanje kontaktnih točaka za europska nadzorna tijela, ESB i svaku državu članicu iz redova relevantnih nacionalnih tijela, koje bi trebalo priopćiti europskim nadzornim tijelima, kako bi se uspostavili glavni sugovornici u koordinacijskom sustavu EU-SCICF-a koje treba obavijestiti u slučaju velikog kiberincidenta. Potrebu za određivanjem kontaktnih točaka trebalo bi procijeniti tijekom razvoja EU-SCICF-a, uzimajući u obzir utvrđenu jedinstvenu kontaktnu točku u skladu s Direktivom (EU) 2016/1148 koju su države članice uspostavile o sigurnosti mrežnih i informacijskih sustava kako bi se osigurala prekogranična suradnja s drugim državama članicama i sa skupinom za suradnju u području mrežne i informacijske sigurnosti ([13]).

(15) Provođenje vježbi upravljanja kriznim i izvanrednim situacijama mogla bi olakšati provedbu EU-SCICF-a i omogućiti tijelima da procijene svoju spremnost i pripravnost za sistemsku kiberkrizu na razini Unije. Takvim bi se vježbama nadležnim tijelima pružila stečena iskustva te bi se omogućilo stalno poboljšanje i razvoj EU-SCICF-a.

([11]) Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016., str. 1.).

([12]) Vidjeti nacrt članka 43. prijedloga DORA-e.

([13]) Vidi Europska komisija, Skupina za suradnju u području mrežne i informacijske sigurnosti, dostupno na mrežnim stranicama Europske komisije na www.ec.europa.eu

(16) Za razvoj EU-SCICF-a ključno je da europska nadzorna tijela zajednički provedu relevantni pripremni rad kako bi se uzeli u obzir mogući ključni elementi okvira i potrebni resursi te potreba za nastavkom njegova razvoja. Nakon toga europska nadzorna tijela mogla bi započeti s radom na preliminarnoj analizi svih prepreka koje bi mogle ometati sposobnosti europskih nadzornih tijela i relevantnih tijela da uspostave EU-SCICF i razmjenjuju relevantne informacije komunikacijskim kanalima u slučaju velikog kiberincidenta. Takva bi analiza bila važan korak u oblikovanju svih daljnjih mjera zakonodavne prirode ili drugih popratnih inicijativa koje Europska komisija može poduzeti u fazi provedbe nakon DORA-e,

DONIJELO JE OVU PREPORUKU:

ODJELJAK 1.

PREPORUKE

Preporuka A – Uspostava paneuropskog okvira za koordinaciju sistemskih kiberincidenata (EU-SCICF)

1. Preporučuje se da se, kako je predviđeno Komisijinim prijedlogom Uredbe Europskog parlamenta i Vijeća o digitalnoj operativnoj otpornosti za financijski sektor (dalje u tekstu „DORA”), europska nadzorna tijela zajedno putem Zajedničkog odbora te zajedno s Europskom središnjom bankom (ESB), Europskim odborom za sistemske rizike (ESRB) i relevantnim nacionalnim tijelima, počnu pripremati za postupni razvoj učinkovitog koordiniranog odgovora na razini Unije u slučaju velikog prekograničnog kiberincidenta ili povezane prijetnje koja bi mogla imati sistemski učinak na financijski sektor Unije. Pripremni rad na koordiniranom odgovoru na razini Unije trebao bi uključivati postupan razvoj EU-SCICF-a za europska nadzorna tijela, ESB, ESRB i relevantna nacionalna tijela. To bi trebalo uključivati i procjenu potrebnih resursa za učinkovit razvoj EU-SCICF-a.

2. Preporučuje se da europska nadzorna tijela, s obzirom na potpreporuku A(1), uz savjetovanje s ESB-om i ESRB-om, provedu pregled i naknadnu analizu trenutačnih zapreka, pravnih i drugih operativnih prepreka učinkovitom razvoju EU-SCICF-a.

Preporuka B – Uspostava kontaktnih točaka EU-SCICF-a

Preporučuje se da europska nadzorna tijela, ESB i svaka država članica iz svojih relevantnih nacionalnih tijela odrede glavnu kontaktnu točku koju bi trebalo priopćiti europskim nadzornim tijelima. Taj popis kontakata olakšat će razvoj okvira i, nakon uspostave EU-SCICF-a, kontaktne točke i ESRB trebali bi biti obaviješteni u slučaju velikog kiberincidenta. Trebalo bi predvidjeti i koordinaciju između EU-SCICF-a i imenovane jedinstvene kontaktne točke u skladu s Direktivom (EU) 2016/1148 koju su države članice uspostavile o sigurnosti mrežnih i informacijskih sustava kako bi se osigurala prekogranična suradnja s drugim državama članicama i sa Skupinom za suradnju u području mrežnih i informacijskih sustava.

Preporuka C – Odgovarajuće mjere na razini Unije

Na temelju rezultata analiza provedenih u skladu s Preporukom A preporučuje se da Komisija razmotri odgovarajuće mjere potrebne za osiguravanje učinkovite koordinacije odgovora na sistemske kiberincidente.

ODJELJAK 2

PROVEDBA

1. **Definicije**

Za potrebe ove Preporuke primjenjuju se sljedeće definicije:

(a) „kiber” znači povezanost, unutar ili preko međusobno povezane informacijske infrastrukture, interakcija među osobama, procesima, podacima i informacijskim sustavima ([14]);

([14]) Vidi Cyber Lexicon, FSB, 12. studenoga 2018., dostupno na internetskim stranicama FSB-a na www.fsb.org.

(b) „veliki kiberincident” znači IKT incident s potencijalno visokim negativnim učinkom na mrežne i informacijske sustave koji podupiru ključne funkcije financijskih subjekata ([15]);

(c) „sistemska kiberkriza” znači veliki kiberincident koji uzrokuje razinu poremećaja u financijskom sustavu Unije koji bi mogao imati ozbiljne negativne posljedice za neometano funkcioniranje unutarnjeg tržišta i realno gospodarstvo. Takva kriza mogla bi biti posljedica velikog kiberincidenta koji uzrokuje šokove u nizu kanala, uključujući operativne, kanale povjerenja i financijske;

(d) „europska nadzorna tijela” ili „ESA-e” znači europsko nadzorno tijelo (Europsko nadzorno tijelo za bankarstvo) osnovano Uredbom (EU) br. 1093/2010 Europskog parlamenta i Vijeća ([16]), zajedno s europskim nadzornim tijelom (Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje) osnovano Uredbom (EU) br. 1094/2010 Europskog parlamenta i Vijeća ([17]) i europskim nadzornim tijelom (Europsko nadzorno tijelo za vrijednosne papire i tržišta kapitala) osnovano Uredbom (EU) br. 1095/2010 Europskog parlamenta i Vijeća ([18]);

(e) „Zajednički odbor” znači Zajednički odbor europskih nadzornih tijela osnovan člankom 54. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 i Uredbe (EU) br. 1095/2010;

(f) „relevantno nacionalno tijelo” znači:

1. nadležno ili nadzorno tijelo u državi članici kako je navedeno u aktima Unije iz članka 1. stavka 2. Uredbe (EU) br. 1093/2010, Uredbe (EU) br. 1094/2010 i Uredbe (EU) br. 1095/2010 te bilo koje drugo nacionalno nadležno tijelo kako je navedeno u aktima Unije kojima se dodjeljuju zadaće europskim nadzornim tijelima;

2. nadležno tijelo u državi članici imenovano u skladu s:

i. člankom 4. Direktive 2013/36/EU Europskog parlamenta i Vijeća ([19]), ne dovodeći u pitanje posebne zadaće dodijeljene ESB-u Uredbom Vijeća (EU) br. 1024/2013 ([20]);

ii. člankom 22. Direktive (EU) 2015/2366 Europskog parlamenta i Vijeća ([21]);

iii. člankom 37. Direktive 2009/110/EZ Europskog parlamenta i Vijeća ([22]);

iv. člankom 4. Direktive (EU) 2019/2034 Europskog parlamenta i Vijeća ([23]);

([15]) Vidi točku 7. nacrta članka 3. prijedloga DORA-e.

([16]) Uredba (EU) br. 1093/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za bankarstvo), kojom se izmjenjuje Odluka br. 716/2009/EZ i stavlja izvan snage Odluka Komisije 2009/78/EZ (SLL 331, 15.12.2010., str. 12.).

([17]) Uredba (EU) br. 1094/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju europskog nadzornog tijela (Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje), o izmjeni Odluke br. 716/2009/EZ i o stavljanju izvan snage Odluke Komisije 2009/79/EZ (SL L 331, 15.12.2010., str. 48.).

([18]) Uredba (EU) br. 1095/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za vrijednosne papire i tržišta kapitala), kojom se izmjenjuje Odluka br. 716/2009/EZ i stavlja izvan snage Odluka Komisije 2009/77/EZ (SL L 331, 15.12.2010., str. 84.).

([19]) Direktiva 2013/36/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama, izmjeni Direktive 2002/87/EZ i stavljanju izvan snage direktiva 2006/48/EZ i 2006/49/EZ (SL L 176, 27.6.2013., str. 338.).

([20]) Uredba Vijeća (EU) br. 1024/2013 od 15. listopada 2013. o dodjeli određenih zadaća Europskoj središnjoj banci u vezi s politikama bonitetnog nadzora kreditnih institucija (SL L 287, 29.10.2013., str. 63.).

([21]) Direktiva (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/EZ (SL L 337, 23.12.2015., str. 35.).

([22]) Direktiva 2009/110/EZ Europskog parlamenta i Vijeća od 16. rujna 2009. o osnivanju, obavljanju djelatnosti i bonitetnom nadzoru poslovanja institucija za elektronički novac te o izmjeni direktiva 2005/60/EZ i 2006/48/EZ i stavljanju izvan snage Direktive 2000/46/EZ (SL L 267, 10.10.2009., str. 7.).

([23]) Direktiva (EU) 2019/2034 Europskog parlamenta i Vijeća od 27. studenoga 2019. o bonitetnom nadzoru nad investicijskim društvima i izmjeni direktiva 2002/87/EZ, 2009/65/EZ, 2011/61/EU, 2013/36/EU, 2014/59/EU i 2014/65/EU (SL L 314, 5.12.2019., str. 64.).

v. člankom 3. stavkom 1. točka (ee) prva alineja Prijedloga uredbe Europskog parlamenta i Vijeća o tržištima kriptoimovine i izmjeni Direktive (EU) 2019/1937 ([24]);

vi. člankom 11. Uredbe (EU) br. 909/2014 Europskog parlamenta i Vijeća ([25]);

vii. člankom 22. Uredbe (EU) br. 648/2012 Europskog parlamenta i Vijeća ([26]);

viii. člankom 67. Direktive 2014/65/EU Europskog parlamenta i Vijeća ([27]);

ix. člankom 22. Uredbe (EU) br. 648/2012;

x. člankom 44. Direktive 2011/61/EU Europskog parlamenta i Vijeća ([28]);

xi. člankom 97. Direktive 2009/65/EC Europskog parlamenta i Vijeća ([29]);

xii. člankom 30. Direktive 2009/138/EC Europskog parlamenta i Vijeća ([30]);

xiii. člankom 12. Direktive (EU) 2016/97 Europskog parlamenta i Vijeća ([31]);

xiv. člankom 47. Direktive (EU) 2016/2341 Europskog parlamenta i Vijeća ([32]);

xv. člankom 22. Uredbe (EC) br. 1060/2009 Europskog parlamenta i Vijeća ([33]);

xvi. člankom 3. stavkom 2. i člankom 32. Direktive 2006/43/EC Europskog parlamenta i Vijeća ([34]);

xvii. člankom 40. Uredbe (EU) 2016/1011 Europskog parlamenta i Vijeća ([35]);

xviii. člankom 29. Uredbe (EU) 2020/1503 Europskog parlamenta i Vijeća ([36]);

([24]) COM (2020) 593 konačno.
([25]) Uredba (EU) br. 909/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o poboljšanju namire vrijednosnih papira u Europskoj uniji i o središnjim depozitorijima vrijednosnih papira te izmjeni direktiva 98/26/EZ i 2014/65/EU te Uredbe (EU) br. 236/2012 (SL L 257, 28.8.2014., str. 1.).
([26]) Uredba (EU) br. 648/2012 Europskog parlamenta i Vijeća od 4. srpnja 2012. o OTC izvedenicama, središnjoj drugoj ugovornoj strani i trgovinskom repozitoriju (SL L 201, 27.7.2012., str. 1.).
([27]) Direktiva 2014/65/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištu financijskih instrumenata i izmjeni Direktive 2002/92/EZ i Direktive 2011/61/EU (SL L 173, 12.6.2014., str. 349.).
([28]) Direktiva 2011/61/EU Europskog parlamenta i Vijeća od 8. lipnja 2011. o upraviteljima alternativnih investicijskih fondova i izmjeni direktiva 2003/41/EZ i 2009/65/EZ te uredbi (EZ) br. 1060/2009 i (EU) br. 1095/2010 (SL L 174, 1.7.2011., str. 1.).
([29]) Direktiva 2009/65/EZ Europskog parlamenta i Vijeća od 13. srpnja 2009. o usklađivanju zakona, uredbi i drugih propisa u odnosu na subjekte za zajednička ulaganja u prenosive vrijednosne papire (UCITS) (SL L 302, 17.11.2009., str. 32.).
([30]) Direktiva 2009/138/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o osnivanju i obavljanju djelatnosti osiguranja i reosiguranja (Solventnost II) (SL L 335, 17.12.2009., str. 1.).
([31]) Direktiva (EU) 2016/97 Europskog parlamenta i Vijeća od 20. siječnja 2016. o distribuciji osiguranja (SL L 26, 2.2.2016., str. 19.).
([32]) Direktiva (EU) 2016/2341 Europskog parlamenta i Vijeća od 14. prosinca 2016. o djelatnostima i nadzoru institucija za strukovno mirovinsko osiguranje (SL L 354, 23.12.2016., str. 37.).
([33]) Uredba (EZ) br. 1060/2009 Europskog parlamenta i Vijeća od 16. rujna 2009. o agencijama za kreditni rejting (SL L 302, 17.11.2009., str. 1.).
([34]) Direktiva 2006/43/EZ Europskog parlamenta i Vijeća od 17. svibnja 2006. o zakonskim revizijama godišnjih financijskih izvještaja i konsolidiranih financijskih izvještaja, kojom se mijenjaju direktive Vijeća 78/660/EEZ i 83/349/EEZ i stavlja izvan snage Direktiva Vijeća 84/253/EEZ (SL L 157, 9.6.2006., str. 87.).
([35]) Uredba (EU) 2016/1011 Europskog parlamenta i Vijeća od 8. lipnja 2016. o indeksima koji se upotrebljavaju kao referentne vrijednosti u financijskim instrumentima i financijskim ugovorima ili za mjerenje uspješnosti investicijskih fondova i o izmjeni direktiva 2008/48/EZ i 2014/17/EU i Uredbe (EU) br. 596/2014 (SL L 171, 29.6.2016., str. 1.).
([36]) Uredba (EU) 2020/1503 Europskog parlamenta i Vijeća od 7. listopada 2020. o europskim pružateljima usluga skupnog financiranja za poduzeća i izmjeni Uredbe (EU) 2017/1129 i Direktive (EU) 2019/1937 (SL L 347, 20.10.2020., str. 1.).

3. tijelo kojem je povjereno donošenje i/ili aktivacija mjera makrobonitetne politike ili drugih zadaća financijske stabilnosti, kao što je povezana popratna analiza, uključujući, ali ne ograničavajući se na:

   i. imenovano tijelo u skladu s glavom VII. poglavljem 4. Direktive 2013/36/EU ili člankom 458. stavkom 1. Uredbe (EU) br. 575/2013 Europskog parlamenta i Vijeća ([37]);

   ii. makrobonitetno tijelo s ciljevima, mehanizmima, zadaćama, ovlastima, instrumentima, zahtjevima u vezi s odgovornošću i drugim svojstvima utvrđenim u Preporuci ESRB/2011/3 Europskog odbora za sistemske rizike ([38]);

(g) „relevantno tijelo" znači:

1. ESA;

2. ESB za zadaće koje su mu dodijeljene u skladu s člankom 4. stavcima 1. i 2. i člankom 5. stavkom 2. Uredbe (EU) br. 1024/2013;

3. relevantno nacionalno tijelo.

2. **Kriteriji za provedbu**

Za provedbu ove Preporuke primjenjuju se sljedeći kriteriji:

(a) trebalo bi voditi računa o načelu nužnosti pristupa informacijama i načelu proporcionalnosti, uzimajući u obzir cilj i sadržaj svake preporuke;

(b) trebali bi biti ispunjeni posebni kriteriji sukladnosti utvrđeni u Prilogu u odnosu na svaku preporuku.

3. **Vremenski okvir za daljnje postupanje**

U skladu s člankom 17. stavkom 1. Uredbe (EU) br. 1092/2010 adresati moraju obavijestiti Europski parlament, Vijeće, Komisiju i ESRB o radnjama poduzetima kao odgovor na ovu Preporuku ili obrazložiti svako nepostupanje. Od primatelja se traži da dostave takvu obavijest u skladu sa sljedećim rokovima:

1. Preporuka A

(a) Od europskih nadzornih tijela traži se da do 30. lipnja 2023., ali ne prije šest mjeseci nakon stupanja na snagu DORA-e, Europskom parlamentu, Vijeću, Komisiji i ESRB-u dostave privremeno izvješće o provedbi potpreporuke A(1).

(b) Od europskih nadzornih tijela traži se da do 30. lipnja 2024., ali ne prije 18 mjeseci nakon stupanja na snagu DORA-e, Europskom parlamentu, Vijeću, Komisiji i ESRB-u dostave završno izvješće o provedbi potpreporuke A(1).

(c) Od europskih nadzornih tijela traži se da do 30. lipnja 2025., ali ne prije 30 mjeseci nakon stupanja na snagu DORA-e, Europskom parlamentu, Vijeću, Komisiji i ESRB-u dostave izvješće o provedbi potpreporuke A(2).

2. Preporuka B

Od europskih nadzornih tijela, ESB-a i država članica traži se da do 30. lipnja 2023., ali ne prije šest mjeseci nakon stupanja na snagu DORA-e, Europskom parlamentu, Vijeću, Komisiji i ESRB-u dostave izvješće o provedbi Preporuke B.

3. Preporuka C

(a) Od Komisije se traži da do 31. prosinca 2023., ali ne prije 12 mjeseci nakon stupanja na snagu DORA-e, Europskom parlamentu, Vijeću i ESRB-u dostavi izvješće o provedbi Preporuke C s obzirom na privremeno izvješće europskih nadzornih tijela u skladu s potpreporukom A(1).

([37]) Uredba (EU) br. 575/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o bonitetnim zahtjevima za kreditne institucije i investicijska društva i o izmjeni Uredbe (EU) br. 648/2012 (SL L 176, 27.6.2013., str. 1.)

([38]) Preporuka ESRB/2011/3 Europskog odbora za sistemske rizike od 22. prosinca 2011. o makrobonitetnim ovlastima nacionalnih tijela (SL C 41, 14.2.2012., str. 1.).

(b) Od Komisije se traži da do 31. prosinca 2025., ali ne prije 36 mjeseci nakon stupanja na snagu DORA-e, Europskom parlamentu, Vijeću i ESRB-u dostavi izvješće o provedbi Preporuke C s obzirom na izvješća europskih nadzornih tijela u skladu s Preporukom A.

4. **Nadzor i ocjena**

1. Tajništvo ESRB-a će:

(a) pomoći adresatima, osiguravanjem koordinacije izvješćivanja i dostavljanjem relevantnih predložaka te, prema potrebi, detaljnim opisivanjem postupka i vremenskog okvira za daljnje postupanje;

(b) provjeravati daljnje postupanje primatelja, pružati pomoć na njihov zahtjev i podnositi izvješća o daljnjim mjerama općem odboru. Procjene će se započeti na sljedeći način:

(i) u roku od 12 mjeseci od stupanja na snagu DORA-e, u pogledu provedbe preporuka A i B;

(ii) u roku od 18 mjeseci od stupanja na snagu DORA-e, u pogledu provedbe Preporuke C;

(iii) u roku od 24 mjeseca od stupanja na snagu DORA-e, u pogledu provedbe Preporuke A;

(iv) u roku od 36 mjeseca od stupanja na snagu DORA-e, u pogledu provedbe Preporuke A;

(v) u roku od 42 mjeseci od stupanja na snagu DORA-e, u pogledu provedbe Preporuke C;

2. Opći odbor će procijeniti radnje i opravdanja o kojima adresati podnose izvješća i, prema potrebi, može utvrditi da se nije postupilo u skladu s ovom Preporukom i da adresat nije dao odgovarajuće obrazloženje za svoje nepostupanje.

Sastavljeno u Frankfurtu na Majni, 2. prosinca 2021.

Voditelj Tajništva ESRB-a,
u ime Općeg odbora ESRB-a,
Francesco MAZZAFERRO

PRILOG

SPECIFIKACIJA KRITERIJA SUKLADNOSTI KOJI SE PRIMJENJUJU NA PREPORUKE

Preporuka A – Uspostava paneuropskog okvira za sistemsku koordinaciju kiberincidenata (EU-SCICF)

Za potpreporuku A(1), navedeni su sljedeći kriteriji usklađenosti.

1. Pri pripremi učinkovitog koordiniranog odgovora na razini Unije koji bi trebao podrazumijevati postupan razvoj EU-SCICF-a izvršavanjem ovlasti predviđene budućom Uredbom Europskog parlamenta i Vijeća o digitalnoj operativnoj otpornosti za financijski sektor (dalje u tekstu „DORA"), europska nadzorna tijela (ESA-e), koja djeluju putem Zajedničkog odbora i zajedno s Europskom središnjom bankom (ESB), Europskim odborom za sistemske rizike (ESRB) i relevantnim nacionalnim tijelima, te uz savjetovanje s Agencijom Europske unije za mrežnu i informacijsku sigurnost i Komisijom, prema potrebi, trebala bi razmotriti uključivanje u predviđenu pripremu za EU-SCICF barem sljedeće aspekte:

   a. analiza potrebnih resursa za učinkovit razvoj EU-SCICF-a;

   b. razvoj vježbi za upravljanje krizama i izvanrednim situacijama koje uključuju scenarije kibernapada s ciljem razvoja komunikacijskih kanala;

   c. razvoj zajedničkog rječnika;

   d. razvoj usklađene klasifikacije kiberincidenata;

   e. uspostava sigurnih i pouzdanih kanala za razmjenu informacija, uključujući sigurnosne sustave;

   f. uspostava kontaktnih točaka;

   g. rješavanje pitanja povjerljivosti u razmjeni informacija;

   h. inicijative za suradnju i razmjenu informacija s obavještajnim podacima financijskog sektora;

   i. razvoj učinkovitih postupaka aktivacije i eskalacije s pomoću informiranosti o stanju;

   j. pojašnjenje odgovornosti sudionika okvira;

   k. razvoj sučelja za međusektorsku koordinaciju i, prema potrebi, koordinaciju trećih zemalja;

   l. osiguravanje usklađene komunikacije relevantnih tijela s javnošću kako bi se očuvalo povjerenje;

   m. uspostava unaprijed definiranih komunikacijskih linija za pravodobnu komunikaciju;

   n. provođenje odgovarajućih vježbi okvirnog testiranja, uključujući međudržavno testiranje i koordinaciju trećih zemalja, te procjene koje rezultiraju stečenim iskustvima i razvojem okvira;

   o. osiguravanje učinkovite komunikacije i protumjera protiv dezinformiranja.

Preporuka B – Uspostava kontaktnih točaka EU-SCICF-a

Za preporuku B navedeni su sljedeći kriteriji sukladnosti.

1. Europska nadzorna tijela, ESB i svaka država članica među svojim relevantnim nacionalnim tijelima trebali bi se dogovoriti o zajedničkom pristupu dijeljenju i ažuriranju popisa određenih kontaktnih točaka EU-SCICF-a.

2. Određivanje kontaktne točke trebalo bi ocijeniti uzimajući u obzir imenovanu jedinstvenu kontaktnu točku na temelju Direktive (EU) 2016/1148 koju su države članice uspostavile u pogledu sigurnosti mrežnih i informacijskih sustava kako bi se osigurala prekogranična suradnja s drugim državama članicama i sa Skupinom za suradnju u području mrežnih i informacijskih sustava.

Preporuka C – Izmjene pravnog okvira Unije

Za preporuku C navodi se sljedeći kriterij sukladnosti.

Komisija bi trebala razmotriti jesu li potrebne bilo kakve mjere, uključujući promjene relevantnog zakonodavstva Unije, kao rezultat analize provedene u skladu s Preporukom A kako bi se osiguralo da europska nadzorna tijela, putem Zajedničkog odbora i zajedno s ESB-om, ESRB-om i relevantnim nacionalnim tijelima, mogu razviti EU-SCICF u skladu s potpreporukom A(1) i kako bi se osiguralo da europska nadzorna tijela, ESB, ESRB i relevantna nacionalna tijela, kao i druga tijela, mogu sudjelovati u koordinacijskim aktivnostima i razmjeni informacija koje su dovoljno detaljne i dosljedne kako bi se pružila potpora djelotvornom EU-SCICF-u.