I

(Rezoliucijos, rekomendacijos ir nuomonės)

REKOMENDACIJOS

EUROPOS SISTEMINĖS RIZIKOS VALDYBA

EUROPOS SISTEMINĖS RIZIKOS VALDYBOS REKOMENDACIJA

2021 m. gruodžio 2 d.

dėl Europos sisteminių kibernetinių incidentų koordinavimo tarp atitinkamų institucijų sistemos

(ESRV/2021/17)

(2022/C 134/01)

EUROPOS SISTEMINĖS RIZIKOS VALDYBOS BENDROJI VALDYBA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į Europos ekonominės erdvės sutartį ([1]), ypač į jos IX priedą,

atsižvelgdama į 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 1092/2010 dėl Europos Sąjungos finansų sistemos makrolygio rizikos ribojimo priežiūros ir Europos sisteminės rizikos valdybos įsteigimo ([2]), ypač į jo 3 straipsnio 2 dalies b ir d punktus ir 16 bei 18 straipsnius,

atsižvelgdama į 2011 m. sausio 20 d. Europos sisteminės rizikos valdybos sprendimą ESRV/2011/1, kuriuo patvirtinamos Europos sisteminės rizikos valdybos darbo tvarkos taisyklės ([3]), ypač į jo 18–20 straipsnius,

kadangi:

(1) kaip pažymėta Europos sisteminės rizikos valdybos rekomendacijos ESRV/2013/1 ([4]) 4 konstatuojamojoje dalyje, galutinis makroprudencinės politikos tikslas yra prisidėti prie visos finansų sistemos stabilumo apsaugos, įskaitant finansų sistemos atsparumo stiprinimą ir sisteminės rizikos susidarymo mažinimą, taip užtikrinant tvarų finansų sektoriaus įnašą į ekonomikos augimą. Europos sisteminės rizikos valdyba (ESRV) yra atsakinga už Sąjungos finansų sistemos makroprudencinę priežiūrą. Vykdydama savo įgaliojimus, ESRV turėtų prisidėti prie sisteminės rizikos finansiniam stabilumui, įskaitant riziką, susijusią su kibernetiniais incidentais, prevencijos ir mažinimo, ir pasiūlyti šios rizikos mažinimo būdus;

(2) dideli kibernetiniai incidentai, atsižvelgiant į jų potencialą sutrikdant ypatingos svarbos finansinių paslaugų teikimą ir operacijų vykdymą, gali kelti sisteminę riziką finansų sistemai. Pirminis sukrėtimas gali sustiprėti dėl veiklos arba finansinio neigiamo poveikio plitimo arba dėl sumažėjusio pasitikėjimo finansų sistema. Jeigu finansų sistema negali absorbuoti šių sukrėtimų, finansiniam stabilumui kyla rizika ir šioje situacijoje gali kilti sisteminė kibernetinė krizė ([5]);

([1]) OL L 1, 1994 1 3, p. 3.
([2]) OL L 331, 2010 12 15, p. 1.
([3]) OL C 58, 2011 2 24, p. 4.
([4]) 2013 m. balandžio 4 d. Europos sisteminės rizikos valdybos rekomendacija ESRV/2013/1 dėl makroprudencinės politikos tarpinių tikslų ir priemonių (OL C 170, 2013 6 15, p. 1).
([5]) Žr. *Systemic cyber risk*, ESRV, 2020 m. vasario mėn., galima rasti ESRV interneto svetainėje www.esrb.europa.eu

(3) nuolat kintanti kibernetinių grėsmių padėtis ir neseniai padidėjęs didelių kibernetinių incidentų skaičius yra padidėjusios rizikos Sąjungos finansiniam stabilumui rodikliai. Per COVID-19 pandemiją išryškėjo svarbus technologijų vaidmuo, kurį jos atlieka sudarant sąlygas veikti finansų sistemai. Atitinkamos institucijos ir įstaigos savo techninę infrastruktūrą ir rizikos valdymo sistemas turi pritaikyti prie staiga padidėjusio nuotolinio darbo masto, dėl kurio finansų sistema apskritai tapo paveikesnė kibernetinėms grėsmėms, o nusikaltėliams atsirado galimybės kurti naujus veikimo būdus ir esamus veikimo būdus pritaikyti siekiant pasinaudoti susidariusia situacija ([6]). Atsižvelgiant į šias aplinkybes, kibernetinių incidentų, apie kuriuos pranešta ECB bankų priežiūros srityje, skaičius 2020 m. padidėjo 54 %, palyginti su 2019 m ([7]).;

(4) įvykus dideliam, galbūt plataus masto, dideliu greičiu ir tempais plintančiam kibernetiniam incidentui, reikia, kad atitinkamos institucijos veiksmingai reaguotų, siekdamos sušvelninti galimas neigiamas pasekmes finansiniam stabilumui. Operatyvus atitinkamų institucijų veiksmų koordinavimas ir komunikacija Sąjungos lygmeniu gali padėti anksti nustatyti didelio kibernetinio incidento poveikį finansiniam stabilumui, išlaikyti pasitikėjimą finansų sistema ir apriboti neigiamų pasekmių išplitimą į kitas finansų įstaigas ir taip padėti užkirsti kelią tam, kad didelis kibernetinis incidentas nekeltų rizikos finansiniam stabilumui;

(5) pagrindinis sukrėtimas atsiranda dėl naujoviškumo, palyginti su įprastomis finansų ir likvidumo krizėmis, su kuriomis paprastai susiduria atitinkamos institucijos. Bendrame rizikos vertinime, be finansinių aspektų, būtina aptarti veiklos sutrikimų mastą ir poveikį, nes jie gali turėti įtakos pasirenkant makroprudencines priemones. Be to, finansinis stabilumas taip pat gali turėti įtakos kibernetikos ekspertų sprendimui, susijusiam su poveikio veiklai mažinimo priemonėmis. Šiuo atveju reikalingas glaudus ir greitas koordinavimas ir atvira komunikacija *inter alia* siekiant gauti informacijos apie padėtį;

(6) nepavykusio institucijų koordinavimo rizika išlieka ir ją reikia pašalinti. Atitinkamos Sąjungos institucijos turės koordinuoti savo veiklą tarpusavyje ir su kitomis institucijomis, pvz., Europos Sąjungos kibernetinio saugumo agentūra (ENISA), su kuriomis jos paprastai nebendrautų. Kadangi nemažai Sąjungos finansų įstaigų veikia pasauliniu mastu, tikėtina, kad didelis kibernetinis incidentas apims ne tik Sąjungos teritoriją arba gali būti pradėtas vykdyti už Sąjungos ribų, todėl atsaką į jį reikėtų koordinuoti pasauliniu mastu;

(7) atitinkamos institucijos turi būti pasirengusios tokiai sąveikai. Priešingu atveju gali kilti rizika, kad jos imsis nesuderintų veiksmų, kurie prieštarauja arba kenkia kitų institucijų atsakui. Dėl tokio nepavykusio koordinavimo finansų sistema gali patirti dar didesnį sukrėtimą, kuris sumažintų pasitikėjimą finansų sistemos veikimu, o tai blogiausiu atveju keltų riziką finansiniam stabilumui ([8]). Todėl, siekiant šalinti finansiniam stabilumui dėl nepavykusio koordinavimo įvykus dideliam kibernetiniam incidentui kylančią riziką, reikėtų imtis būtinų veiksmų;

(8) ESRV (2021) ataskaitoje *Mitigating systemic cyber risk* ([9]) nustatytas poreikis sukurti Europos sisteminių kibernetinių incidentų koordinavimo tarp atitinkamų Sąjungos institucijų sistemą (angl. *pan-European systemic cyber incident coordination framework*, toliau – EU-SCICF). EU-SCICF paskirtis turėtų būti padidinti atitinkamų institucijų parengties lygį, siekiant palengvinti koordinuotą atsaką į galimą didelį kibernetinį incidentą. ESRV (2021) ataskaitoje *Mitigating systemic cyber risk* numatyta, kad ESRV įvertina sistemos ypatumus, kurių prireiktų *prima facie* nesėkmingo koordinavimo rizikai pašalinti;

(9) pagrindinis šios rekomendacijos tikslas – pasinaudoti viena iš Europos Parlamento ir Tarybos pasiūlyme dėl Reglamento dėl skaitmeninės veiklos atsparumo finansų sektoriuje ([10]) (toliau – DORA) nustatytų Europos priežiūros institucijų (EPI) funkcijų, t. y. palaipsniui sudaryti sąlygas veiksmingam Sąjungos lygmens koordinuotam atsakui įvykus dideliam tarpvalstybiniam informacijos ir ryšių technologijų (IRT) incidentui arba kilus susijusiai grėsmei, kuri daro sisteminį poveikį visam Sąjungos finansų sektoriui. Šio proceso metu bus sukurta atitinkamų institucijų EU-SCICF;

([6]) Žr. organizuoto nusikalstamumo internete grėsmės vertinimą, Europolas, 2020 m., galima rasti Europolo interneto svetainėje www.europol.europa.eu

([7]) Žr. *IT and cyber risk: a constant challenge*, ECB, 2021 m., galima rasti ECB bankininkystės priežiūros interneto svetainėje www.bankingsupervision.europa.eu

([8]) Žr. *Systemic cyber risk*, ESRV, 2020 m. vasario mėn., galima rasti ESRV interneto svetainėje www.esrb.europa.eu

([9]) Žr. *Mitigating systemic cyber risk*, ESRV, 2021 m. (bus paskelbta).

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

(10) EU-SCICF turėtų būti siekiama ne pakeisti esamas sistemas, bet pašalinti bet kokias koordinavimo ir komunikavimo spragas tarp pačių atitinkamų institucijų ir su kitomis Sąjungos institucijomis bei kitais pagrindiniais dalyviais tarptautiniu lygmeniu. Šiuo atžvilgiu reikėtų įvertinti EU-SCICF vietą dabartinėje finansų krizės sistemoje ir išsamioje Sąjungos kibernetinių incidentų sistemoje. Dėl pačių atitinkamų institucijų koordinavimo pažymėtina, kad, be kita ko, reikėtų atsižvelgti į finansų sektoriaus subjektų tinklo ir informacinių sistemų (TIS) bendradarbiavimo grupės funkcijas ir veiklą pagal Europos Parlamento ir Tarybos direktyvą (ES) 2016/1148 ([11]), ir koordinavimo mechanizmus, kuriuos numatyta sukurti įsteigiant Jungtinį kibernetinio saugumo padalinį, įskaitant ENISA dalyvavimą;

(11) visų pirma pasiūlymu pradėti EU-SCICF rengimo darbus siekiama patvirtinti galimas EPI funkcijas, numatytas DORA pasiūlyme. DORA siūloma, kad „EPI, pasitarusios jungtiniame komitete ir bendradarbiaudamos su kompetentingomis institucijomis, Europos Centriniu Banku (ECB) ir ESRV, gali nustatyti mechanizmus, kurie sudarytų sąlygas dalytis veiksminga praktika skirtinguose finansų sektoriuose, kad būtų didinamas informuotumas apie padėtį ir identifikuojami bendri kibernetiniai pažeidžiamumai ir rizika įvairiuose sektoriuose“ ir „gali parengti krizių valdymo ir nenumatytų atvejų užduotis, apimančias kibernetinių išpuolių scenarijus, siekdamos sukurti komunikacijos kanalus ir palaipsniui sudaryti sąlygas veiksmingam ES lygmens koordinuotam atsakui didelio tarpvalstybinio IRT incidento ar susijusios grėsmės, turinčios sisteminį poveikį visam Sąjungos finansų sektoriui, atveju“ ([12]). Tokios Europos sistemos kaip EU-SCICF dar nėra ir ją reikėtų sukurti ir plėtoti kartu su DORA;

(12) atsižvelgiant į riziką finansiniam stabilumui Sąjungoje, kurią kelia kibernetinė rizika, parengiamuosius darbus, susijusius su EU-SCICF sukūrimu, reikėtų, kiek tai įmanoma, pradėti net prieš tai, kai bus visapusiškai taikoma jai sukurti reikalinga teisinė ir politinė sistema. Ši teisinė ir politinė sistema turėtų būti visiškai sukurta ir užbaigta pradėjus taikyti atitinkamas DORA nuostatas ir jos deleguotuosius aktus;

(13) veiksminga komunikacija padeda atitinkamoms institucijoms gauti informacijos apie padėtį, taigi tai yra būtinoji sąlyga Sąjungos lygmens koordinavimui įvykus dideliems kibernetiniams incidentams. Šiuo atžvilgiu reikėtų apibrėžti komunikacijos infrastruktūrą, reikalingą atsakui į didelį kibernetinį incidentą koordinuoti. Tai reikštų poreikį nurodyti informacijos, kuria reikia dalytis, tipą, įprastus kanalus, naudojamus dalijantis tokia informacija, ir informacinius centrus, su kuriais tokia informacija reikėtų dalytis. Dalijantis informacija būtina laikytis galiojančių teisinių reikalavimų. Be to, atitinkamoms institucijoms gali prireikti apibrėžti veiksmų planą ir protokolus, kuriais reikia vadovautis, siekiant užtikrinti tinkamą institucijų, dalyvaujančių planuojant koordinuotą atsaką į didelį kibernetinį incidentą, koordinavimą;

(14) sisteminės kibernetinės krizės atveju reikės pradėti visapusiškai bendradarbiauti nacionaliniu ir Sąjungos lygmenimis. Todėl EPI ir ECB informacinių centrų paskyrimas ir kiekvienos valstybės narės atitinkamų nacionalinių institucijų kaip informacinių centrų paskyrimas, apie kuriuos reikėtų pranešti EPI, gali būti numatytas siekiant EU-SCICF schemoje sukurti pagrindinius ryšių palaikymo punktus, kuriuos reikia informuoti didelio kibernetinio incidento atveju. Poreikį paskirti informacinius centrus reikėtų įvertinti EU-SCICF kūrimo metu, atsižvelgiant į paskirtą bendrąjį informacinį centrą tinklo ir informacinių sistemų saugumo klausimais pagal Direktyvą (ES) 2016/1148, kurį valstybės narės įsteigė siekdamos užtikrinti tarpvalstybinį bendradarbiavimą su kitomis valstybėmis narėmis ir TIS bendradarbiavimo grupe ([13]);

(15) elgesys valdant krizę ir nenumatytų atvejų užduotys galėtų palengvinti EU-SCICF įgyvendinimą ir sudaryti sąlygas institucijoms įvertinti jų pasirengimą ir parengtį sisteminei kibernetinei krizei Sąjungos lygmeniu. Tokios užduotys padėtų institucijoms įgyti patirties ir sudarytų sąlygas nuolat tobulinti ir plėsti EU-SCICF;

([11]) 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL L 194, 2016 7 19, p. 1).

([12]) Žr. DORA pasiūlymo 43 straipsnio projektą.

([13]) Žr. informaciją apie Europos Komisijos TIS bendradarbiavimo grupę, kurią galima rasti Europos Komisijos interneto svetainėje ec.europa.eu

(16) kuriant EU-SCICF labai svarbu, kad EPI kartu atliktų susijusius parengiamuosius darbus ir išnagrinėtų galimus pagrindinius sistemos elementus ir reikalingus išteklius bei poreikius, kad sistemą būtų galima plėtoti toliau. Paskui EPI galėtų imtis darbų, susijusių su preliminaria bet kokių kliūčių, dėl kurių galėtų sumažėti EPI ir atitinkamų institucijų gebėjimai sukurti EU-SCICF ir dalytis susijusia informacija per komunikacijos kanalus didelio kibernetinio incidento atveju, analize. Tokia analizė būtų svarbus žingsnis pagrindžiant bet kokius tolesnius veiksmus, susijusius su teisėkūra arba kitomis pagalbinėmis iniciatyvomis, kurių Europos Komisija gali imtis po DORA įgyvendinimo etapo,

PRIĖMĖ ŠIĄ REKOMENDACIJĄ:

1 SKIRSNIS

REKOMENDACIJOS

A rekomendacija. Europos sisteminių kibernetinių incidentų koordinavimo sistemos (EU-SCICF) sukūrimas

1. Rekomenduojama, kad, kaip numatyta Europos Parlamento ir tarybos pasiūlyme dėl Reglamento dėl skaitmeninės veiklos atsparumo finansų sektoriuje (toliau – DORA), Europos priežiūros institucijos (EPI) kartu per jungtinį komitetą ir drauge su Europos Centriniu Banku (ECB), Europos sisteminės rizikos valdyba (ESRV) ir atitinkamomis nacionalinėmis institucijomis pradėtų rengtis palaipsniui kurti veiksmingą Sąjungos lygmens koordinuotą atsaką didelio tarpvalstybinio kibernetinio incidento arba susijusios grėsmės, kuri galėtų daryti sisteminį poveikį Sąjungos finansų sektoriui, atveju. Parengiamieji darbai, susiję su Sąjungos lygmens koordinuotu atsaku, turėtų apimti laipsnišką EPI, ECB, ESRV ir atitinkamų nacionalinių institucijų EU-SCICF kūrimą. Šiuo atveju taip pat reikėtų įvertinti išteklių reikalavimus, susijusius su veiksmingu EU-SCICF kūrimu.

2. Rekomenduojama, kad EPI, atsižvelgdamos į A rekomendacijos 1 punktą ir pasikonsultavusios su ECB ir ESRV, nustatytų ir paskui išanalizuotų dabartines kliūtis, teisines ir kitas veiklos spragas, trukdančias veiksmingai kurti EU-SCICF.

B rekomendacija. EU-SCICF informacinių centrų sukūrimas

Rekomenduojama, kad EPI, ECB ir kiekviena valstybė narė iš savo atitinkamų nacionalinių institucijų turėtų paskirti pagrindinį informacinį centrą, apie kurį reikėtų pranešti EPI. Šis informacinių centrų sąrašas padės kurti sistemą ir, kai EU-SCICF bus sukurta, informacinius centrus ir ESRV reikėtų informuoti apie didelio kibernetinio incidento atvejį. Taip pat reikėtų numatyti koordinavimą tarp EU-SCICF ir paskirtojo bendrojo informacinio centro tinklo ir informacinių sistemų saugumo klausimais pagal Direktyvą (ES) 2016/1148, kurį valstybės narės įsteigė siekdamos užtikrinti tarpvalstybinį bendradarbiavimą su kitomis valstybėmis narėmis ir tinklo ir informacinių sistemų bendradarbiavimo grupe.

C rekomendacija. Tinkamos Sąjungos lygmens priemonės

Rekomenduojama, kad Komisija, remdamasi pagal A rekomendaciją atliktų analizių rezultatu, apsvarstytų tinkamas priemones, kurios būtų reikalingos veiksmingam atsako į sisteminius kibernetinius incidentus koordinavimui užtikrinti.

2 SKIRSNIS

ĮGYVENDINIMAS

1. **Apibrėžtys**

Šioje rekomendacijoje taikomos tokios apibrėžtys:

a) kibernetinis – susijęs su tarpusavyje sujungtos informacinės infrastruktūros, kurioje vyksta asmenų, procesų, duomenų ir informacinių sistemų sąveika, laikmena, esantis jos viduje arba perduodamas per ją ([14]);

([14]) Žr. *Cyber Lexicon*, FSB, 2018 m. lapkričio 12 d., galima rasti FSB interneto svetainėje www.fsb.org

b) didelis kibernetinis incidentas – su IRT susijęs incidentas, galintis turėti didelį neigiamą poveikį tinklui ir informacinėms sistemoms, kurios padeda finansų sektoriaus subjektams vykdyti ypatingos svarbos funkcijas ([15]);

c) sisteminė kibernetinė krizė – didelis kibernetinis incidentas, kuris Sąjungos finansų sistemoje sukelia tokio lygmens sutrikimą, dėl kurio gali atsirasti rimtos neigiamos pasekmės sklandžiam vidaus rinkos ir realiosios ekonomikos veikimui. Tokia krizė galėtų atsirasti dėl didelio kibernetinio incidento, kuris sukelia sukrėtimus įvairiuose kanaluose, įskaitant veiklos, konfidencialumo ir finansinį kanalus;

d) Europos priežiūros institucijos (EPI) – Europos priežiūros institucija (Europos bankininkystės institucija), įsteigta Europos Parlamento ir Tarybos reglamentu (ES) Nr. 1093/2010 ([16]), taip pat Europos priežiūros institucija (Europos draudimo ir profesinių pensijų institucija), įsteigta Europos Parlamento ir Tarybos reglamentu (ES) Nr. 1094/2010 ([17]), ir Europos priežiūros institucija (Europos vertybinių popierių ir rinkų institucija), įsteigta Europos Parlamento ir Tarybos reglamentu (ES) Nr. 1095/2010 ([18]);

e) jungtinis komitetas – Europos priežiūros institucijų jungtinis komitetas, įsteigtas pagal Reglamento (ES) Nr. 1093/2010, Reglamento (ES) Nr. 1094/2010 ir Reglamento (ES) Nr. 1095/2010 54 straipsnį;

f) atitinkamos nacionalinės institucijos –

1) valstybės narės kompetentinga arba priežiūros institucija, kaip nurodyta Sąjungos aktuose, į kuriuos nuoroda pateikta Reglamento (ES) Nr. 1093/2010, Reglamento (ES) Nr. 1094/2010 ir Reglamento (ES) Nr. 1095/2010 1 straipsnio 2 dalyje ir bet kuri kita nacionalinė kompetentinga institucija, kaip nurodyta Sąjungos aktuose, kuriais pavedamos užduotys EPI;

2) kompetentinga institucija, valstybėje narėje paskirta pagal:

i) Europos Parlamento ir Tarybos direktyvos 2013/36/ES ([19]) 4 straipsnį, nedarant poveikio konkrečioms užduotims, kurios ECB pavestos pagal Tarybos reglamento (ES) Nr. 1024/2013 ([20]);

ii) Europos Parlamento ir Tarybos direktyvos (ES) 2015/2366 22 straipsnis ([21]);

iii) Europos Parlamento ir Tarybos direktyvos (ES) 2009/110/EB 37 straipsnis ([22]);

iv) Europos Parlamento ir Tarybos direktyvos (ES) 2019/2034 4 straipsnis ([23]);

([15]) Žr. DORA pasiūlymo 3 straipsnio projekto 7 punktą.

([16]) 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1093/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos bankininkystės institucija), iš dalies keičiamas Sprendimas Nr. 716/2009/EB ir panaikinamas Komisijos sprendimas 2009/78/EB (OL L 331, 2010 12 15, p. 12).

([17]) 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1094/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos draudimo ir profesinių pensijų institucija), iš dalies keičiamas Sprendimas Nr. 716/2009/EB ir panaikinamas Komisijos sprendimas 2009/79/EB (OL L 331, 2010 12 15, p. 48).

([18]) 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1095/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos vertybinių popierių ir rinkų institucija) ir iš dalies keičiamas Sprendimas Nr. 716/2009/EB bei panaikinamas Komisijos sprendimas 2009/77/EB (OL L 331, 2010 12 15, p. 84).

([19]) 2013 m. birželio 26 d. Europos Parlamento ir Tarybos direktyva 2013/36/ES dėl galimybės verstis kredito įstaigų veikla ir dėl riziką ribojančios kredito įstaigų priežiūros, kuria iš dalies keičiama Direktyva 2002/87/EB ir panaikinamos direktyvos 2006/48/EB bei 2006/49/EB (OL L 176, 2013 6 27, p. 338).

([20]) 2013 m. spalio 15 d. Tarybos reglamentas (ES) Nr. 1024/2013, kuriuo Europos Centriniam Bankui pavedami specialūs uždaviniai, susiję su rizikos ribojimu pagrįstos kredito įstaigų priežiūros politika (OL L 287, 2013 10 29, p. 63).

([21]) 2015 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva (ES) 2015/2366 dėl mokėjimo paslaugų vidaus rinkoje, kuria iš dalies keičiamos direktyvos 2002/65/EB, 2009/110/EB ir 2013/36/ES bei Reglamentas (ES) Nr. 1093/2010 ir panaikinama Direktyva 2007/64/EB (OL L 337, 2015 12 23, p. 35).

([22]) 2009 m. rugsėjo 16 d. Europos Parlamento ir Tarybos direktyva 2009/110/EB dėl elektroninių pinigų įstaigų steigimosi, veiklos ir riziką ribojančios priežiūros, iš dalies keičianti direktyvas 2005/60/EB ir 2006/48/EB ir panaikinanti Direktyvą 2000/46/EB (OL L 267, 2009 10 10, p. 7).

([23]) 2019 m. lapkričio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2019/2034 dėl investicinių įmonių riziką ribojančios priežiūros, kuria iš dalies keičiamos direktyvos 2002/87/EB, 2009/65/EB, 2011/61/ES, 2013/36/ES, 2014/59/ES ir 2014/65/ES (OL L 314, 2019 12 5, p. 64).

v) Pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl kriptoturto rinkų, kuriuo iš dalies keičiama Direktyva (ES) 2019/1937 ([24]) 3 straipsnio 1 dalies ee punkto pirma įtrauka;

vi) Europos Parlamento ir Tarybos reglamento (ES) 909/2014 11 straipsnis ([25]);

vii) Europos Parlamento ir Tarybos reglamento (ES) 648/2012 22 straipsnis ([26]);

viii) Europos Parlamento ir Tarybos direktyvos 2014/65/ES 67 straipsnis ([27]);

ix) Reglamento (ES) Nr. 648/2012 22 straipsnis;

x) Europos Parlamento ir Tarybos direktyvos 2011/61/ES 44 straipsnis ([28]);

xi) Europos Parlamento ir Tarybos direktyvos 2009/65/EB 97 straipsnis ([29]);

xii) Europos Parlamento ir Tarybos direktyvos 2009/138/EB 30 straipsnis ([30]);

xiii) Europos Parlamento ir Tarybos direktyvos (ES) 2016/97 12 straipsnis ([31]);

xiv) Europos Parlamento ir Tarybos direktyvos (ES) 2016/2341 47 straipsnis ([32]);

xv) Europos Parlamento ir Tarybos reglamento (EB) Nr. 1060/2009 22 straipsnis ([33]);

xvi) Europos Parlamento ir Tarybos direktyvos 2006/43/EB ([34]) 3 straipsnio 2 dalis ir 32 straipsnis;

xvii) Europos Parlamento ir Tarybos reglamento (ES) 2016/1011 ([35]) 40 straipsnis;

xviii) Europos Parlamento ir Tarybos reglamento (ES) 2020/1503 ([36]) 29 straipsnis;

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

([25]) 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 909/2014 dėl atsiskaitymo už vertybinius popierius gerinimo Europos Sąjungoje ir centrinių vertybinių popierių depozitoriumų, kuriuo iš dalies keičiamos direktyvos 98/26/EB ir 2014/65/ES bei Reglamentas (ES) Nr. 236/2012 (OL L 257, 2014 8 28, p. 1).

([26]) 2012 m. liepos 4 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 648/2012 dėl ne biržos išvestinių finansinių priemonių, pagrindinių sandorio šalių ir sandorių duomenų saugyklų (OL L 201, 2012 7 27, p. 1).

([27]) 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos direktyva 2014/65/ES dėl finansinių priemonių rinkų, kuria iš dalies keičiamos Direktyva 2002/92/EB ir Direktyva 2011/61/ES (OL L 173, 2014 6 12, p. 349).

([28]) 2011 m. birželio 8 d. Europos Parlamento ir Tarybos direktyva 2011/61/ES dėl alternatyvaus investavimo fondų valdytojų, kuria iš dalies keičiami direktyvos 2003/41/EB ir 2009/65/EB bei reglamentai (EB) Nr. 1060/2009 ir (ES) Nr. 1095/2010 (OL L 174, 2011 7 1, p. 1).

([29]) 2009 m. liepos 13 d. Europos Parlamento ir Tarybos direktyva 2009/65/EB dėl įstatymų ir kitų teisės aktų, susijusių su kolektyvinio investavimo į perleidžiamus vertybinius popierius subjektais (KIPVPS), derinimo (OL L 302, 2009 11 17, p. 32).

([30]) 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/138/EB dėl draudimo ir perdraudimo veiklos pradėjimo ir jos vykdymo (Mokumas II) (OL L 335, 2009 12 17, p. 1).

([31]) 2016 m. sausio 20 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/97 dėl draudimo produktų platinimo (OL L 26, 2016 2 2, p. 19).

([32]) 2016 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/2341 dėl profesinių pensijų įstaigų (PPĮ) veiklos ir priežiūros (OL L 354, 2016 12 23, p. 37).

([33]) 2009 m. rugsėjo 16 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1060/2009 dėl kredito reitingų agentūrų (OL L 302, 2009 11 17, p. 1).

([34]) 2006 m. gegužės 17 d. Europos Parlamento ir Tarybos direktyva 2006/43/EB dėl teisės aktų nustatyto metinės finansinės atskaitomybės ir konsoliduotos finansinės atskaitomybės audito, iš dalies keičianti Tarybos direktyvas 78/660/EEB ir 83/349/EEB bei panaikinanti Tarybos direktyvą 84/253/EEB (OL L 157, 2006 6 9, p. 87).

([35]) 2016 m. birželio 8 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 2016/1011 dėl indeksų, kurie kaip lyginamieji indeksai naudojami finansinėse priemonėse ir finansinėse sutartyse arba siekiant įvertinti investicinių fondų veiklos rezultatus, kuriuo iš dalies keičiami direktyvos 2008/48/EB ir 2014/17/ES bei Reglamentas (ES) Nr. 596/2014 (OL L 171, 2016 6 29, p. 1).

([36]) 2020 m. spalio 7 d. Europos Parlamento ir Tarybos reglamentas (ES) 2020/1503 dėl Europos sutelktinio finansavimo paslaugų verslui teikėjų, kuriuo iš dalies keičiamas Reglamentas (ES) 2017/1129 ir Direktyva (ES) 2019/1937 (OL L 347, 2020 10 20, p. 1).

3) institucija, kuriai pavesta patvirtinti ir (arba) aktyvuoti makroprudencinės politikos priemones arba kitos finansinio stabilumo užtikrinimo užduotys, pvz., susijusios su pagalbine analize, be kita ko, įskaitant:

i) paskirtąją instituciją pagal Direktyvos 2013/36/ES VII antraštinės dalies 4 skyrių arba Europos Parlamento ir Tarybos reglamentą (ES) Nr. 575/2013 ([37]) 458 straipsnio 1 dalį;

ii) makroprudencinės priežiūros įstaigą, turinčią tikslus, susitarimus, užduotis, įgaliojimus, priemones, atskaitomybės reikalavimus ir kitus Europos sisteminės rizikos valdybos rekomendacijoje ESRV/2011/3 nustatytus ypatumus ([38]);

g) atitinkama institucija –

1) EPI;

2) ECB, atsižvelgiant į užduotis, pavestas jam pagal Reglamento (ES) Nr. 1024/2013 4 straipsnio 1 ir 2 dalis ir 5 straipsnio 2 dalį;

3) atitinkama nacionalinė institucija.

2. **Įgyvendinimo kriterijai**

Įgyvendinant šią rekomendaciją, taikomi šie kriterijai:

a) tinkamą dėmesį reikėtų skirti poreikiui žinoti ir proporcingumo principui, atsižvelgiant į rekomendacijos tikslą ir turinį;

b) turėtų būti įvykdyti su kiekviena rekomendacija susiję priede išvardyti konkretūs atitikties kriterijai.

3. **Tolesnių veiksmų tvarkaraštis**

Pagal Reglamento (ES) Nr. 1092/2010 17 straipsnio 1 dalį adresatai privalo pranešti Europos Parlamentui, Tarybai, Komisijai ir ESRV apie veiksmus, kurių jie ėmėsi šiai rekomendacijai įgyvendinti, arba pagrįsti bet kokį neveikimą. Adresatų prašoma tokį pranešimą dėl atitikties pateikti laikantis šių terminų:

1. A rekomendacija

a) Iki 2023 m. birželio 30 d., bet ne anksčiau kaip praėjus šešiems mėnesiams nuo DORA įsigaliojimo, EPI prašoma pateikti Europos Parlamentui, Tarybai, Komisijai ir ESRV tarpinę A rekomendacijos 1 dalies įgyvendinimo ataskaitą.

b) Iki 2024 m. birželio 30 d., bet ne anksčiau kaip praėjus 18 mėnesių nuo DORA įsigaliojimo, EPI prašoma pateikti Europos Parlamentui, Tarybai, Komisijai ir ESRV galutinę A rekomendacijos 1 dalies įgyvendinimo ataskaitą.

c) Iki 2025 m. birželio 30 d., bet ne anksčiau kaip praėjus 30 mėnesių nuo DORA įsigaliojimo, EPI prašoma pateikti Europos Parlamentui, Tarybai, Komisijai ir ESRV A rekomendacijos 2 dalies įgyvendinimo ataskaitą.

2. B rekomendacija

Iki 2023 m. birželio 30 d., bet ne anksčiau kaip praėjus šešiems mėnesiams nuo DORA įsigaliojimo, EPI, ECB ir valstybių narių prašoma pateikti Europos Parlamentui, Tarybai, Komisijai ir ESRV B rekomendacijos įgyvendinimo ataskaitą.

3. C rekomendacija

a) Iki 2023 m. gruodžio 31 d., bet ne anksčiau kaip praėjus 12 mėnesių nuo DORA įsigaliojimo, Komisijos prašoma pateikti Europos Parlamentui, Tarybai, Komisijai ir ESRV C rekomendacijos įgyvendinimo ataskaitą, atsižvelgiant į EPI tarpinę ataskaitą, pateiktą pagal A rekomendacijos 1 dalį.

([37]) 2013 m. birželio 26 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 575/2013 dėl prudencinių reikalavimų kredito įstaigoms ir investicinėms įmonėms ir kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 648/2012 (OL L 176, 2013 6 27, p. 1).

([38]) 2011 m. gruodžio 22 d. Europos sisteminės rizikos valdybos rekomendacija ESRV/2011/3 dėl nacionalinių institucijų įgaliojimų makrolygio rizikos ribojimo srityje (OL C 41, 2012 2 14, p. 1).

b) Iki 2025 m. gruodžio 31 d., bet ne anksčiau kaip praėjus 36 mėnesių nuo DORA įsigaliojimo, Komisijos prašoma pateikti Europos Parlamentui, Tarybai, Komisijai ir ESRV C rekomendacijos įgyvendinimo ataskaitas, atsižvelgiant į EPI ataskaitas, pateiktas pagal A rekomendaciją.

4. **Stebėsena ir vertinimas**

1. ESRV sekretoriatas:

a) padės adresatams užtikrindamas koordinuotą pranešimų teikimą ir parengdamas atitinkamas formas, taip pat prireikus išsamiai aprašydamas procedūrą ir tolesnių veiksmų tvarkaraštį;

b) patikrins, kokių tolesnių veiksmų ėmėsi adresatai, teiks pagalbą jiems paprašius ir Bendrajai valdybai teiks ataskaitas apie tolesnius veiksmus. Vertinimai bus pradedami tokia tvarka:

i) per 12 mėnesių, įsigaliojus DORA dėl A ir B rekomendacijų įgyvendinimo;

ii) per 18 mėnesių, įsigaliojus DORA dėl C rekomendacijos įgyvendinimo;

iii) per 24 mėnesius, įsigaliojus DORA dėl A rekomendacijos įgyvendinimo;

iv) per 36 mėnesius, įsigaliojus DORA dėl A rekomendacijos įgyvendinimo;

v) per 42 mėnesių, įsigaliojus DORA dėl C rekomendacijos įgyvendinimo.

2. Bendroji valdyba įvertins adresatų pranešimą apie veiksmus ir pateiktą pagrindimą ir, kai tinkama, gali nuspręsti, kad šios rekomendacijos nebuvo laikomasi ir kad adresatas nesugebėjo tinkamai pagrįsti savo neveikimo.

Priimta Frankfurte prie Maino 2021 m. gruodžio 2 d.

ESRV bendrosios valdybos vardu
ESRV sekretoriato vadovas
Francesco MAZZAFERRO

PRIEDAS

REKOMENDACIJOMS TAIKOMŲ ATITIKTIES KRITERIJŲ SPECIFIKACIJA

A rekomendacija. Europos sisteminių kibernetinių incidentų koordinavimo sistemos (EU-SCICF) sukūrimas

Dėl A rekomendacijos 1 dalies teikiama ši atitikties kriterijų specifikacija.

1. Rengdamos veiksmingą Sąjungos lygmens koordinuotą atsaką, kuris turėtų apimti laipsnišką EU-SCICF kūrimą įgyvendinant būsimame Europos Parlamento ir Tarybos reglamente dėl skaitmeninės veiklos atsparumo finansų sektoriuje (toliau – DORA) numatytus įgaliojimus, Europos priežiūros institucijos (EPI), veikdamos jungtiniame komitete ir drauge su Europos Centriniu Banku (ECB), Europos sisteminės rizikos valdyba (ESRV) ir atitinkamomis nacionalinėmis institucijomis, taip pat pasikonsultavusios su Europos Sąjungos tinklų ir informacijos apsaugos agentūra ir prireikus Komisija, turėtų apsvarstyti galimybę į numatytus EU-SCICF parengiamuosius darbus įtraukti bent jau šiuos aspektus:

   a) veiksmingam EU-SCICF kūrimui reikalingų išteklių analizę;

   b) krizės valdymo ir nenumatytų atvejų užduočių, susijusių su kibernetinio išpuolio scenarijais, parengimą siekiant tobulinti komunikacijos kanalus;

   c) parengti bendrą žodyną;

   d) nustatyti išsamią kibernetinių incidentų klasifikaciją;

   e) sukurti saugius ir patikimus dalijimosi informacija kanalus, įskaitant atsargines sistemas;

   f) įsteigti informacinius centrus;

   g) aptarti konfidencialumo dalijantis informacija klausimus;

   h) bendradarbiavimo ir dalijimosi informacija su finansų sektoriaus kibernetine žvalgyba iniciatyvas;

   i) pasinaudojant informuotumu apie padėtį, parengti veiksmingus aktyvavimo ir eskalacijos procesus;

   j) patikslinti sistemos dalyvių pareigas;

   k) parengti tarpsektorinio ir, kai tinkama, trečiųjų šalių koordinavimo sąsajas;

   l) užtikrinti nuoseklią atitinkamų institucijų komunikaciją su visuomene, siekiant išlaikyti pasitikėjimą;

   m) sukurti iš anksto nustatytas komunikacijos linijas, kad būtų užtikrinta savalaikė komunikacija;

   n) atlikti tinkamas sistemos testavimo užduotis, įskaitant tarpvalstybinį testavimą ir trečiųjų šalių koordinavimą, taip pat atlikti vertinimus, kurie padėtų įgyti patirties ir tobulinti sistemą;

   o) užtikrinti veiksmingą komunikaciją ir kovos su dezinformacija priemones.

B rekomendacija. EU-SCICF informacinių centrų sukūrimas

Dėl B rekomendacijos teikiama ši atitikties kriterijų specifikacija.

1. EPI, ECB ir kiekviena valstybė narė su savo atitinkamomis nacionalinėmis institucijomis turėtų susitarti dėl bendro požiūrio į dalijimąsi EU-SCICF paskirtųjų informacinių centrų sąrašu ir jo atnaujinimą.

2. Informacinio punkto paskyrimas turėtų būti įvertintas atsižvelgiant į paskirtojo bendrojo informacinio centro pagal Direktyvą (ES) 2016/1148, kurį valstybės narės įsteigė siekdamos užtikrinti tarpvalstybinį bendradarbiavimą su kitomis valstybėmis narėmis ir tinklo ir informacinių sistemų bendradarbiavimo grupe.

C rekomendacija. Sąjungos teisinės sistemos pakeitimai

Dėl C rekomendacijos teikiama ši atitikties kriterijaus specifikacija.

Komisija turėtų įvertinti, ar bet kokios priemonės, įskaitant atitinkamų Sąjungos teisės aktų pakeitimus, yra reikalingos atsižvelgiant į pagal A rekomendaciją atliktą analizę siekiant užtikrinti, kad EPI kartu su jungtiniu komitetu ir drauge su ECB, ESRV ir atitinkamomis nacionalinėmis institucijomis, galėtų sukurti EU-SCICF pagal A rekomendacijos 1 dalį ir užtikrinti, kad EPI, ECB, ESRV ir atitinkamos nacionalinės institucijos, taip pat kitos institucijos galėtų dalyvauti vykdant koordinavimo veiksmus ir keistis informacija, kuri yra pakankamai išsami ir nuosekli, kad būtų remiamas veiksmingas EU-SCICF veikimas.