I

(Rezolūcijas, ieteikumi un atzinumi)

IETEIKUMI

EIROPAS SISTĒMISKO RISKU PADOME

EIROPAS SISTĒMISKO RISKU KOLĒĢIJAS IETEIKUMS

(2021. gada 2. decembris)

par sistēmisku kiberincidentu Eiropas līmeņa koordinācijas mehānismu attiecīgajām iestādēm

(ESRK/2021/17)

(2022/C 134/01)

EIROPAS SISTĒMISKO RISKU KOLĒĢIJAS VALDE,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Līgumu par Eiropas Ekonomikas zonu ([1]) un jo īpaši tā IX pielikumu,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1092/2010 (2010. gada 24. novembris) par Eiropas Savienības finanšu sistēmas makrouzraudzību un Eiropas Sistēmisko risku kolēģijas izveidošanu ([2]) un jo īpaši tās 3. panta 2. punkta b) un d) apakšpunktu, kā arī 16. un 18. pantu,

ņemot vērā Eiropas Sistēmisko risku kolēģijas Lēmumu ESRK/2011/1 (2011. gada 20. janvāris), ar ko pieņem Eiropas Sistēmisko risku kolēģijas Reglamentu ([3]), un jo īpaši tā 18.–20. pantu,

tā kā:

(1) Kā norādīts Eiropas Sistēmisko risku kolēģijas Ieteikuma ESRK/2013/1 ([4]) 4. apsvērumā, makroprudenciālās uzraudzības politikas galvenais mērķis ir garantēt finanšu sistēmas stabilitāti kopumā, tai skaitā stiprinot finanšu sistēmas noturību un mazinot sistēmisko risku veidošanos, tādējādi nodrošinot finanšu sektora ieguldījumu tautsaimniecības izaugsmē. Eiropas Sistēmisko risku kolēģija (ESRK) atbild par Eiropas Savienības finanšu sistēmas makroprudenciālo uzraudzību. Īstenojot savas pilnvaras, ESRK būtu jāpalīdz novērst un mazināt sistēmiskos riskus finanšu stabilitātei, tostarp tos, kas saistīti ar kiberincidentiem, un jāierosina, kā šos riskus varētu mazināt.

(2) Nozīmīgi kiberincidenti var radīt sistēmisku risku finanšu sistēmai, ņemot vērā to potenciālu traucēt kritiski svarīgus finanšu pakalpojumus un operācijas. Sākotnējā satricinājuma pastiprināšanās var notikt vai nu ar operacionālā vai finanšu kaitējuma izplatības palīdzību, vai arī mazinot uzticību finanšu sistēmai. Ja finanšu sistēma nespēs absorbēt šos satricinājumus, finanšu stabilitāte būs apdraudēta, un šāda situācija var izraisīt sistēmisku kiberkrīzi ([5]).

([1]) OV L 1, 3.1.1994., 3. lpp.
([2]) OV L 331, 15.12.2010., 1. lpp.
([3]) OV C 58, 24.2.2011., 4. lpp.
([4]) Eiropas Sistēmisko risku kolēģijas Ieteikums ESRK/2013/1 (2013. gada 4. aprīlis) par makrouzraudzības politikas vidēja termiņa mērķiem un instrumentiem (OV C 170, 15.6.2013., 1. lpp.).
([5]) Sk. *Systemic cyber risk*, ESRK, 2020. gada februāris, pieejams ESRK interneta vietnē www.esrb.europa.eu

(3) Pastāvīgi mainīgā kiberdraudu vide un nesenais nozīmīgu kiberincidentu pieaugums liecina par lielāku risku finanšu stabilitātei Eiropas Savienībā. Covid-19 pandēmija izgaismojusi tehnoloģiju nozīmi finanšu sistēmas darbības nodrošināšanā. Attiecīgajām varasiestādēm un institūcijām bija jāpielāgo sava tehniskā infrastruktūra un riska pārvaldības sistēmas attālinātā darba pēkšņam pieaugumam, kas palielinājis finanšu sistēmas vispārējo pakļautību kiberdraudiem un ļāvis noziedzniekiem gan izstrādāt jaunus darbības veidus, gan pielāgot esošos, lai izmantotu situāciju ([6]). Ņemot vērā iepriekš minēto, 2020. gadā ECB banku uzraudzībai paziņoto kiberincidentu skaits palielinājās par 54 % salīdzinājumā ar 2019. gadu ([7]).

(4) Nozīmīga kiberincidenta potenciāli plašā mēroga, ātruma un izplatības dēļ attiecīgajām iestādēm efektīvi jāreaģē, lai mazinātu iespējamo negatīvo ietekmi uz finanšu stabilitāti. Ātra koordinācija un saziņa starp attiecīgajām iestādēm Savienības līmenī var palīdzēt laikus novērtēt nozīmīga kiberincidenta ietekmi uz finanšu stabilitāti, saglabājot uzticību finanšu sistēmai un ierobežojot kaitējuma izplatību uz citām finanšu iestādēm, tādējādi palīdzot novērst to, ka nozīmīgs kiberincidents kļūst par risku finanšu stabilitātei.

(5) Satricinājumi rodas jaunā veidā, kas atšķiras no tradicionālajām finanšu un likviditātes krīzēm, ar kurām parasti saskaras attiecīgās iestādes. Papildus finansiālajiem aspektiem vispārējā riska novērtējumā jāiekļauj darbības traucējumu mērogs un ietekme, jo tie var ietekmēt makroprudenciālo instrumentu izvēli. Tāpat arī finanšu stabilitāte varētu ietekmēt kiberspeciālistu izvēli attiecībā uz operacionāliem riska mazināšanas faktoriem. Tādēļ vajadzīga cieša un ātra koordinācija un atklāta saziņa, lai cita starpā veicinātu situācijas apzināšanos.

(6) Pastāv risks, ka iestādes nespēj nodrošināt koordināciju, un šādu risku ir jānovērš. Attiecīgajām iestādēm Savienībā būs jāsadarbojas savā starpā un ar citām iestādēm, piemēram, ar Eiropas Savienības Tīklu un informācijas drošības aģentūru (ENISA), ar kuru tās parasti iespējams nesadarbojas. Tā kā ievērojams skaits Savienības finanšu iestāžu darbojas visā pasaulē, nozīmīgs kiberincidents, visticamāk, nebūs saistīts tikai ar Savienību vai varētu tikt uzsākts ārpus Savienības, un tam varētu būt nepieciešama globāla reaģēšanas koordinācija.

(7) Attiecīgajām iestādēm jābūt gatavām šādai mijiedarbībai. Pretējā gadījumā tās varētu riskēt veikt nekonsekventas darbības, kas ir pretrunā ar citu iestāžu atbildēm vai apdraud tās. Šāda koordinācijas kļūda varētu pastiprināt finanšu sistēmas šoku, izraisot uzticības mazināšanos finanšu sistēmas darbībai, kas sliktākajā gadījumā radītu risku finanšu stabilitātei ([8]). Tādēļ būtu jāveic vajadzīgie pasākumi, lai novērstu risku finanšu stabilitātei, kas izriet no koordinācijas kļūdas nozīmīga kiberincidenta gadījumā.

(8) ESRK 2021. gada ziņojumā *Sistēmiskā kiberriska mazināšana* ([9]) konstatēta nepieciešamība izveidot sistēmisku kiberincidentu Eiropas līmeņa koordinācijas mehānismu (EU-SCICF) attiecīgajām iestādēm Savienībā. EU-SCICF mērķis būtu palielināt attiecīgo iestāžu sagatavotību, lai veicinātu koordinētu reakciju uz potenciāli nozīmīgu kiberincidentu. ESRK 2021. gada ziņojumā *Sistēmiskā kiberriska mazināšana* sniegts ESRK novērtējums par galvenajām iezīmēm, kas prima facie būtu vajadzīgas, lai novērstu koordinācijas kļūdas risku.

(9) Šā ieteikuma galvenais mērķis ir balstīties uz vienu no Eiropas uzraudzības iestāžu (EUI) funkcijām, kas paredzētas priekšlikumā Eiropas Parlamenta un Padomes regulai par finanšu sektora digitālās darbības noturību ([10]) (turpmāk –"DORA"), proti, pakāpeniski nodrošināt efektīvu un koordinētu Savienības līmeņa reakciju gadījumā, ja rodas nozīmīgs ar informācijas un komunikācijas tehnoloģijām (IKT) saistīts incidents vai saistīts apdraudējums, kam ir sistēmiska ietekme uz Savienības finanšu nozari kopumā. Šā procesa rezultātā attiecīgajām iestādēm tiks izveidots EU-SCICF.

([6]) Sk. *Internet Organised Crime Threat Assessment*, Eiropols, 2020. gads, pieejams Eiropola interneta vietnē www.europol.europa.eu
([7]) Sk. *IT and cyber risk: a constant challenge*, ECB, 2021. gads, pieejams ECB banku uzraudzības interneta vietnē www.bankingsupervision.europa.eu
([8]) Sk. *Systemic cyber risk*, ESRK, 2020. gada februāris, pieejams ESRK tīmekļa vietnē www.esrb.europa.eu
([9]) Sk. *Mitigating systemic cyber risk*, ESRK, 2021. gads, (vēl nav publicēts).
([10]) COM/2020/595 final.

(10) EU-SCICF mērķim nevajadzētu būt aizstāt esošos mehānismus, bet gan novērst jebkādas koordinācijas un saziņas nepilnības starp attiecīgajām iestādēm un citām iestādēm Savienībā, un citiem galvenajiem dalībniekiem starptautiskā līmenī. Šajā sakarā būtu jāapsver EU-SCICF vieta pašreizējā finanšu krīžu regulējumā un Savienības kiberincidentu regulējuma kontekstā. Attiecībā uz koordināciju starp pašām attiecīgajām iestādēm būtu jāapsver, bet ne tikai, Eiropas Parlamenta un Padomes Direktīvā (ES) 2016/1148 ([11]) paredzētās Tīkla un informācijas sistēmu (TIS) sadarbības grupas finanšu vienību jautājumos loma un darbības, kā arī koordinācijas mehānismi, kas paredzēti, izveidojot Kopīgu kibervienību līdztekus ENISA iesaistei.

(11) Jo īpaši priekšlikuma sākt EU-SCICF sagatavošanu mērķis ir apstiprināt EUI potenciālās lomas, kā paredzēts DORA priekšlikumā. DORA ierosināts, ka "EUI ar Apvienotās komitejas starpniecību un sadarbībā ar kompetentajām iestādēm, Eiropas Centrālo banku (ECB) un ESRK var izveidot mehānismus, kas ļautu apmainīties ar efektīvu praksi starp finanšu nozarēm, lai uzlabotu situācijas apzināšanos un apzinātu kopējus kibernoturības un riskus dažādās nozarēs", un "var izstrādāt krīzes pārvarēšanas un ārkārtas situācijas mācības, kas ietver kiberuzbrukumu scenārijus, lai attīstītu saziņas kanālus un pakāpeniski nodrošinātu efektīvu un koordinētu ES līmeņa reakciju gadījumos, kad rodas būtisks pārrobežu ar IKT saistīts incidents vai saistīts apdraudējums, kam ir sistēmiska ietekme uz Savienības finanšu nozari kopumā" ([12]). Tāds Eiropas līmeņa mehānisms kā EU-SCICF vēl nepastāv, un tas būtu jāizveido un jāattīsta DORA kontekstā.

(12) Ņemot vērā risku Savienības finanšu stabilitātei, ko rada kiberrisks, sagatavošanās darbiem EU-SCICF pakāpeniskai izveidei, ciktāl tas iespējams, būtu jāsākas pat pirms tā izveidei nepieciešamā tiesiskā un politiskā regulējuma pilnīgas piemērošanas. Šis tiesiskais un politikas regulējums tiktu pilnībā pabeigts, tiklīdz būs piemērojami attiecīgie DORA un tās deleģēto aktu noteikumi.

(13) Efektīva saziņa veicina situācijas apzināšanos starp attiecīgajām iestādēm un tādējādi ir obligāts priekšnoteikums Savienības mēroga koordinācijai nozīmīgu kiberincidentu laikā. Šajā sakarā būtu jādefinē komunikācijas infrastruktūra, kas vajadzīga, lai koordinētu reakciju uz nozīmīgu kiberincidentu. Tas nozīmētu, ka būtu jāprecizē sniegtās informācijas veids, šādas informācijas apmaiņas parastie kanāli un kontaktpunkti, kuriem informācija būtu jāsniedz. Sniedzot informāciju, jāievēro spēkā esošās juridiskās prasības. Turklāt attiecīgajām iestādēm, iespējams, būs jāizstrādā skaidrs rīcības plāns un protokoli, kas jāievēro, lai nodrošinātu pienācīgu koordināciju starp iestādēm, kas iesaistītas, plānojot koordinētu reakciju uz nozīmīgu kiberincidentu.

(14) Sistēmiska kiberkrīze prasīs uzsākt pilnīgu sadarbību nacionālā un Savienības līmenī. Tāpēc EUI, ECB un katras dalībvalsts kontaktpunktu izraudzīšanos no to attiecīgo nacionālo iestāžu vidus, par ko būtu jāpaziņo EUI, var paredzēt, lai izveidotu tos galvenos sarunu partnerus EU-SCICF koordinācijas shēmā, kurus būtu jāinformē nozīmīga kiberincidenta gadījumā. Nepieciešamība izraudzīties kontaktpunktus būtu jāizvērtē EU-SCICF izveides laikā, ņemot vērā vienoto kontaktpunktu saskaņā ar Direktīvu (ES) 2016/1148, ko dalībvalstis izveidojušas tīklu un informācijas sistēmu drošības jomā, lai nodrošinātu pārrobežu sadarbību ar citām dalībvalstīm un TIS sadarbības grupu ([13]).

(15) Krīžu pārvarēšanas un ārkārtas mācību veikšana varētu atvieglot EU-SCICF īstenošanu un ļaut iestādēm izvērtēt savu gatavību un gatavību sistēmiskai kiberkrīzei Savienības līmenī. Šādas mācības sniegtu iestādēm pieredzi un ļautu pastāvīgi uzlabot un pilnveidot EU-SCICF.

([11]) Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194, 19.7.2016., 1. lpp.).

([12]) Sk. DORA priekšlikuma 43. panta projektu.

([13]) Sk. Eiropas Komisijas TIS sadarbības grupa, pieejams Eiropas Komisijas interneta vietnē ec.europa.eu

(16) Lai attīstītu EU-SCICF, ir būtiski, ka EUI kopīgi veic attiecīgos sagatavošanas darbus, lai apsvērtu sistēmas iespējamos galvenos elementus un vajadzīgos resursus, un lai turpinātu tā izstrādi. Pēc tam EUI varētu sākt sākotnējo analīzi par jebkādiem šķēršļiem, kas varētu kavēt EUI un attiecīgo iestāžu spēju izveidot EU-SCICF un nozīmīga kiberincidenta gadījumā apmainīties ar attiecīgo informāciju izmantojot saziņas kanālus. Šāda analīze būtu svarīgs solis, lai informētu par jebkādām turpmākajām darbībām likumdošanas vai citu atbalstošo iniciatīvu veidā, ko Eiropas Komisija varētu veikt DORA īstenošanas posmā,

IR PIEŅĒMUSI ŠO IETEIKUMU.

1. IEDAĻA

IETEIKUMI

A ieteikums. Sistēmisku kiberincidentu Eiropas līmeņa koordinācijas mehānisma (EU-SCICF) izveide

1. Kā paredzēts Komisijas priekšlikumā Eiropas Parlamenta un Padomes regulai par finanšu sektora digitālās darbības noturību (turpmāk – "DORA"), Eiropas uzraudzības iestādēm (EUI) ar Apvienotās komitejas starpniecību un kopā ar Eiropas Centrālo banku (ECB), Eiropas Sistēmisko risku kolēģiju (ESRK) un attiecīgajām nacionālajām iestādēm tiek ieteikts sākt gatavoties pakāpeniskai efektīvas Savienības līmeņa koordinētas reakcijas izstrādei gadījumā, ja rodas nozīmīgs pārrobežu kiberincidents vai saistīts apdraudējums, kas varētu sistēmiski ietekmēt Savienības finanšu nozari. Sagatavošanās darbiem, kas vērsti uz Savienības līmeņa koordinētu reakciju, būtu jāietver EU-SCICF pakāpeniska attīstība attiecībā uz EUI, ECB, ESRK un attiecīgajām nacionālajām iestādēm. Tiem būtu jāiekļauj arī novērtējums par resursu vajadzībām, lai efektīvi attīstītu EU-SCICF.

2. Ņemot vērā A ieteikuma 1. punktu, EUI, apspriežoties ar ECB un ESRK, ieteicams veikt pašreizējo šķēršļu, juridisko un citu operacionālo ierobežojumu kartēšanu un turpmāku analīzi EU-SCICF efektīvai attīstībai.

B ieteikums. EU-SCICF kontaktpunktu izveide

Tiek ieteikts EUI, ECB un katrai dalībvalstij, izvēloties kādu no savām attiecīgajām nacionālajām iestādēm, norīkot galveno kontaktpunktu, par kuru būtu jāpaziņo EUI. Šāds kontaktpersonu saraksts atvieglos regulējuma izstrādi, un, tiklīdz būs izveidots EU-SCICF, kontaktpunkti un ESRK būtu jāinformē par nozīmīgiem kiberincidentiem. Būtu jāparedz arī koordinācija starp EU-SCICF un izraudzīto vienoto kontaktpunktu saskaņā ar Direktīvu (ES) 2016/1148, ko dalībvalstis izveidojušas tīklu un informācijas sistēmu drošības jomā, lai nodrošinātu pārrobežu sadarbību ar citām dalībvalstīm un Tīklu un informācijas sistēmu sadarbības grupu.

C ieteikums. Atbilstīgi pasākumi Savienības līmenī

Pamatojoties uz saskaņā ar A ieteikumu veikto analīžu rezultātiem, Komisijai tiek ieteikts apsvērt piemērotus pasākumus, kas vajadzīgi, lai nodrošinātu efektīvu koordināciju reakcijai uz sistēmiskiem kiberincidentiem.

2. IEDAĻA

ĪSTENOŠANA

1. **Definīcijas**

Šajā ieteikumā piemēro šādas definīcijas:

a) "kibernētisks" ir saistīts ar savstarpēji savienotu informācijas infrastruktūru, kas ietver mijiedarbību starp personām, procesiem, datiem un informācijas sistēmām, vai iekļauts tajā vai darbojas ar tās palīdzību ([14]);

([14]) Sk. *Cyber Lexicon*, FSP, 2018. gada 12. novembris, pieejams FSP interneta vietnē www.fsb.org

b) "nozīmīgs kiberincidents" ir ar IKT saistīts incidents ar potenciāli lielu negatīvu ietekmi uz tīklu un informācijas sistēmām, kas atbalsta finanšu iestāžu kritiski svarīgās funkcijas ([15]);

c) "sistēmiska kiberkrīze" ir nozīmīgs kiberincidents, kas izraisa tik lielus traucējumus Savienības finanšu sistēmā, kas var radīt nopietnas negatīvas sekas iekšējā tirgus netraucētai darbībai un reālās tautsaimniecības darbībai. Šādu krīzi varētu izraisīt nozīmīgs kiberincidents, kas izraisītu satricinājumus vairākos kanālos, tostarp operacionālajos, uzticības un finanšu kanālos;

d) "Eiropas Uzraudzības iestādes" jeb "EUI" ir Eiropas Uzraudzības iestāde (Eiropas Banku iestāde), kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1093/2010 ([16]), kopā ar Eiropas Uzraudzības iestādi (Eiropas Apdrošināšanas un aroda pensiju iestādi), kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1094/2010 ([17]), un Eiropas Uzraudzības iestādi (Eiropas Vērtspapīru un tirgu iestādi), kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1095/2010 ([18]);

e) "Apvienotā komiteja" ir Eiropas Uzraudzības iestāžu apvienotā komiteja, kas izveidota ar Regulas (ES) Nr. 1093/2010, Regulas (ES) Nr. 1094/2010 un Regulas (ES) Nr. 1095/2010 54. pantu;

f) "attiecīgā nacionālā iestāde" ir:

1. kompetentā vai uzraudzības iestāde dalībvalstī, kas noteikta Savienības aktos, kuri minēti Regulas (ES) Nr. 1093/2010, Regulas (ES) Nr. 1094/2010 un Regulas (ES) Nr. 1095/2010 1. panta 2. punktā, un jebkura cita nacionālā kompetentā iestāde, kas noteikta Savienības aktos, ar kuriem uztic uzdevumus EUI;

2. dalībvalsts kompetentā iestāde, kas norīkota saskaņā ar:

i. Eiropas Parlamenta un Padomes Direktīvas 2013/36/ES ([19]) 4. pantu, neskarot īpašos uzdevumus, kas ECB uzticēti ar Padomes Regulu (ES) Nr. 1024/2013 ([20]);

ii. Eiropas Parlamenta un Padomes Direktīvas (ES) 2015/2366 ([21]) 22. pantu;

iii. Eiropas Parlamenta un Padomes Direktīvas 2009/110/EK ([22]) 37. pantu;

iv. Eiropas Parlamenta un Padomes Direktīvas (ES) 2019/2034 ([23]) 4. pantu;

([15]) Sk. DORA priekšlikuma 3. panta 7) punkta projektu.

([16]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 1093/2010 (2010. gada 24. novembris), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Banku iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/78/EK (OV L 331, 15.12.2010., 12. lpp.).

([17]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 1094/2010 (2010. gada 24. novembris), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Apdrošināšanas un fondēto pensiju iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/79/EK (OV L 331, 15.12.2010., 48. lpp.).

([18]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 1095/2010 (2010. gada 24. novembris), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Vērtspapīru un tirgu iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/77/EK (OV L 331, 15.12.2010., 84. lpp.).

([19]) Eiropas Parlamenta un Padomes Direktīva 2013/36/ES (2013. gada 26. jūnijs) par piekļuvi kredītiestāžu darbībai un kredītiestāžu prudenciālo uzraudzību, ar ko groza Direktīvu 2002/87/EK un atceļ Direktīvas 2006/48/EK un 2006/49/EK (OV L 176, 27.6.2013., 338. lpp.).

([20]) Padomes Regula (ES) Nr. 1024/2013 (2013. gada 15. oktobris), ar ko Eiropas Centrālajai bankai uztic īpašus uzdevumus saistībā ar politikas nostādnēm, kas attiecas uz kredītiestāžu prudenciālo uzraudzību (OV L 287, 29.10.2013., 63. lpp.).

([21]) Eiropas Parlamenta un Padomes Direktīva (ES) 2015/2366 (2015. gada 25. novembris) par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/ES un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK (OV L 337, 23.12.2015., 35. lpp.).

([22]) Eiropas Parlamenta un Padomes Direktīva 2009/110/EK (2009. gada 16. septembris) par elektroniskās naudas iestāžu darbības sākšanu, veikšanu un konsultatīvu uzraudzību, par grozījumiem Direktīvā 2005/60/EK un Direktīvā 2006/48/EK un par Direktīvas 2000/46/EK atcelšanu (OV L 267, 10.10.2009., 7. lpp.).

([23]) Eiropas Parlamenta un Padomes Direktīva (ES) 2019/2034 (2019. gada 27. novembris) par ieguldījumu brokeru sabiedrību prudenciālo uzraudzību un ar ko groza Direktīvas 2002/87/EK, 2009/65/EK, 2011/61/ES, 2013/36/ES, 2014/59/ES un 2014/65/ES (OV L 314, 5.12.2019., 64. lpp.).

v. priekšlikuma Eiropas Parlamenta un Padomes Regulai par kriptoaktīvu tirgiem un ar ko groza Direktīvu (ES) 2019/1937 ([24]) 3. panta 1. punkta ee) apakšpunkta pirmo ievilkumu;

vi. Eiropas Parlamenta un Padomes Regulas (ES) Nr. 909/2014 ([25]) 11. pantu;

vii. Eiropas Parlamenta un Padomes Regulas (ES) Nr. 648/2012 ([26]) 22. pantu;

viii. Eiropas Parlamenta un Padomes Direktīvas 2014/65/ES ([27]) 67. pantu;

ix. Regulas (ES) Nr. 648/2012 22. pantu;

x. Eiropas Parlamenta un Padomes Direktīvas 2011/61/ES ([28]) 44. pantu;

xi. Eiropas Parlamenta un Padomes Direktīvas 2009/65/EK ([29]) 97. pantu;

xii. Eiropas Parlamenta un Padomes Direktīvas 2009/138/EK ([30]) 30. pantu;

xiii. Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/97 ([31]) 12. pantu;

xiv. Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/2341 ([32]) 47. pantu;

xv. Eiropas Parlamenta un Padomes Regulas (EK) Nr. 1060/2009 ([33]) 22. pantu;

xvi. Eiropas Parlamenta un Padomes Direktīvas 2006/43/EK ([34]) 3. panta 2. punktu un 32. pantu;

xvii. Eiropas Parlamenta un Padomes Regulas (ES) 2016/1011 ([35]) 40. pants;

xviii. Eiropas Parlamenta un Padomes Regulas (ES) 2020/1503 ([36]) 29. pants;

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

([25]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 909/2014 (2014. gada 23. jūlijs) par vērtspapīru norēķinu uzlabošanu Eiropas Savienībā, centrālajiem vērtspapīru depozitārijiem un grozījumiem Direktīvās 98/26/EK un 2014/65/ES un Regulā (ES) Nr. 236/2012 (OV L 257, 28.8.2014., 1. lpp.).

([26]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 648/2012 (2012. gada 4. jūlijs) par ārpusbiržas atvasinātajiem instrumentiem, centrālajiem darījumu partneriem un darījumu reģistriem (OV L 201, 27.7.2012., 1. lpp.).

([27]) Eiropas Parlamenta un Padomes Direktīva 2014/65/ES (2014. gada 15. maijs) par finanšu instrumentu tirgiem un ar ko groza Direktīvu 2002/92/ES un Direktīvu 2011/61/ES (OV L 173, 12.6.2014., 349. lpp.).

([28]) Eiropas Parlamenta un Padomes 2011. gada 8. jūnija Direktīva 2011/61/ES par alternatīvo ieguldījumu fondu pārvaldniekiem un par grozījumiem Direktīvā 2003/41/EK, Direktīvā 2009/65/EK, Regulā (EK) Nr. 1060/2009 un Regulā (ES) Nr. 1095/2010 (OV L 174, 1.7.2011., 1. lpp.).

([29]) Eiropas Parlamenta un Padomes Direktīva 2009/65/EK (2009. gada 13. jūlijs) par normatīvo un administratīvo aktu koordināciju attiecībā uz pārvedamu vērtspapīru kolektīvo ieguldījumu uzņēmumiem (PVKIU) (OV L 302, 17.11.2009., 32. lpp.).

([30]) Eiropas Parlamenta un Padomes Direktīva 2009/138/EK (2009. gada 25. novembris) par uzņēmējdarbības uzsākšanu un veikšanu apdrošināšanas un pārapdrošināšanas jomā (Maksātspēja II) (OV L 335, 17.12.2009., 1. lpp.).

([31]) Eiropas Parlamenta un Padomes Direktīva (ES) 2016/97 (2016. gada 20. janvāris) par apdrošināšanas izplatīšanu (OV L 26, 2.2.2016. , 19. lpp.).

([32]) Eiropas Parlamenta un Padomes Direktīva (ES) 2016/2341 (2016. gada 14. decembris) par arodpensijas kapitāla uzkrāšanas institūciju (AKUI) darbību un uzraudzību (OV L 354, 23.12.2016., 37. lpp.).

([33]) Eiropas Parlamenta un Padomes Regula (EK) Nr. 1060/2009 (2009. gada 16. septembris) par kredītreitinga aģentūrām (OV L 302, 17.11.2009., 1. lpp.).

([34]) Eiropas Parlamenta un Padomes Direktīva 2006/43/EK (2006. gada 17. maijs), ar ko paredz gada pārskatu un konsolidēto pārskatu obligātās revīzijas, groza Padomes Direktīvu 78/660/EEK un Padomes Direktīvu 83/349/EEK un atceļ Padomes Direktīvu 84/253/EEK (OV L 157, 9.6.2006., 87. lpp.).

([35]) Eiropas Parlamenta un Padomes Regula (ES) 2016/1011 (2016. gada 8. jūnijs) par indeksiem, ko izmanto kā etalonus finanšu instrumentos un finanšu līgumos vai ieguldījumu fondu darbības rezultātu mērīšanai, un ar kuru groza Direktīvu 2008/48/EK, Direktīvu 2014/17/ES un Regulu (ES) Nr. 596/2014 (OV L 171, 29.6.2016., 1. lpp.).

([36]) Eiropas Parlamenta un Padomes Regula (ES) 2020/1503 (2020. gada 7. oktobris) par Eiropas kolektīvās finansēšanas pakalpojumu sniedzējiem uzņēmējdarbībai un ar ko groza Regulu (ES) 2017/1129 un Direktīvu (ES) 2019/1937 (OV L 347, 20.10.2020., 1. lpp.).

3. iestāde, kurai uzticēta makroprudenciālās uzraudzības politikas pasākumu vai citu ar finanšu stabilitāti saistītu uzdevumu veikšana un/vai aktivizēšana, piemēram, ar to saistīta atbalsta analīze, tostarp, bet ne tikai:

   i. norīkotā iestāde saskaņā ar Direktīvas 2013/36/ES VII sadaļas 4. nodaļu vai Eiropas Parlamenta un Padomes Regulas (ES) Nr. 575/2013 ([37]) 458. panta 1. punktu;

   ii. makroprudenciālās uzraudzības iestāde, kuras mērķi, regulējums, uzdevumi, pilnvaras, instrumenti, atbildības prasības un citas īpašības izklāstītas Eiropas Sistēmisko risku kolēģijas Ieteikumā ESRK/2011/3 ([38]);

g) "attiecīgā iestāde" ir:

   1. EUI;

   2. ECB attiecībā uz uzdevumiem, kas tai uzticēti saskaņā ar Regulas (ES) Nr. 1024/2013 4. panta 1. un 2. punktu un 5. panta 2. punktu;

   3. attiecīgā nacionālā iestāde.

2. **Īstenošanas kritēriji**

Uz šī ieteikuma īstenošanu attiecas šādi kritēriji:

a) pienācīga vērība jāpievērš vajadzības pēc informācijas principam un proporcionalitātes principam, ņemot vērā katra ieteikuma mērķi un saturu;

b) jāizpilda īpašie atbilstības kritēriji, kas izklāstīti pielikumā attiecībā uz katru ieteikumu.

3. **Pārskatu sniegšanas termiņi**

Saskaņā ar Regulas (ES) Nr. 1092/2010 17. panta 1. punktu adresātiem jāinformē Eiropas Parlaments, Padome, Komisija un ESRK par darbībām, kas veiktas, reaģējot uz šo ieteikumu, vai jāpamato jebkāda bezdarbība. Adresātiem jāsniedz šādi paziņojumi, ievērojot šādus termiņus.

1. A ieteikums

   a) Līdz 2023. gada 30. jūnijam, bet ne agrāk kā sešus mēnešus pēc DORA stāšanās spēkā, EUI tiek lūgts iesniegt Eiropas Parlamentam, Padomei, Komisijai un ESRK starpposma pārskatu par A ieteikuma 1. punkta īstenošanu.

   b) Līdz 2024. gada 30. jūnijam, bet ne agrāk kā 18 mēnešus pēc DORA stāšanās spēkā, EUI tiek lūgts iesniegt Eiropas Parlamentam, Padomei, Komisijai un ESRK galīgo pārskatu par A ieteikuma 1. punkta īstenošanu.

   c) Līdz 2025. gada 30. jūnijam, bet ne agrāk kā 30 mēnešus pēc DORA stāšanās spēkā, EUI tiek lūgts iesniegt Eiropas Parlamentam, Padomei, Komisijai un ESRK pārskatu par A ieteikuma 2. punkta īstenošanu.

2. B ieteikums

   Līdz 2023. gada 30. jūnijam, bet ne agrāk kā sešus mēnešus pēc DORA stāšanās spēkā, EUI, ECB un dalībvalstīm tiek lūgts iesniegt Eiropas Parlamentam, Padomei, Komisijai un ESRK pārskatu par B ieteikuma īstenošanu.

3. C ieteikums

   a) Līdz 2023. gada 31. decembrim, bet ne agrāk kā 12 mēnešus pēc DORA stāšanās spēkā, Komisijai tiek lūgts iesniegt Eiropas Parlamentam, Padomei un ESRK pārskatu par C ieteikuma īstenošanu, ņemot vērā EUI starpposma pārskatu saskaņā ar A ieteikuma 1. punktu.

([37]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 575/2013 (2013. gada 26. jūnijs) par prudenciālajām prasībām attiecībā uz kredītiestādēm un ieguldījumu brokeru sabiedrībām, un ar ko groza Regulu (ES) Nr. 648/2012 (OV L 176, 27.6.2013., 1. lpp.).

([38]) Eiropas Sistēmisko risku kolēģijas Ieteikums ESRK/2011/13 (2011. gada 22. decembris) par nacionālo iestāžu pilnvarām makrouzraudzības jomā (OV C 41, 14.2.2012., 1. lpp.).

b) Līdz 2025. gada 31. decembrim, bet ne agrāk kā 36 mēnešus pēc DORA stāšanās spēkā, Komisijai tiek lūgts iesniegt Eiropas Parlamentam, Padomei un ESRK pārskatu par C ieteikuma īstenošanu, ņemot vērā EUI pārskatus saskaņā ar A ieteikumu.

4. **Monitorēšana un novērtējums**

1. ESRK Sekretariāts:

a) palīdz adresātiem, t.sk., nodrošinot koordinētu pārskatu sniegšanu un nodrošinot attiecīgus paraugus, un vajadzības gadījumā precizējot pārskatu sniegšanas kārtību un grafiku;

b) pārbauda, vai adresāti izpilda ieteikumus, t.sk., pēc to lūguma sniedzot palīdzību adresātiem, un sniedz pārskatu par izpildi ESRK Valdei. Novērtējumus uzsāk šādi:

i) 12 mēnešu laikā pēc DORA stāšanās spēkā attiecībā uz A un B ieteikuma īstenošanu;

ii) 18 mēnešu laikā pēc DORA stāšanās spēkā attiecībā uz C ieteikuma īstenošanu;

iii) 24 mēnešu laikā pēc DORA stāšanās spēkā attiecībā uz A ieteikuma īstenošanu;

iv) 36 mēnešu laikā pēc DORA stāšanās spēkā attiecībā uz A ieteikuma īstenošanu;

v) 42 mēnešu laikā pēc DORA stāšanās spēkā attiecībā uz C ieteikuma īstenošanu;

2. ESRK Valde izvērtēs darbības un pamatojumus, par kuriem paziņojuši adresāti, un vajadzības gadījumā var lemt par to, ka šis ieteikums nav ievērots un adresāti nav pienācīgi pamatojuši savu bezdarbību.

Frankfurtē pie Mainas, 2021. gada 2. decembrī

ESRK Valdes vārdā –
ESRK sekretariāta vadītājs
Francesco MAZZAFERRO

PIELIKUMS

IETEIKUMIEM PIEMĒROJAMO ATBILSTĪBAS KRITĒRIJU APRAKSTS

A ieteikums. Sistēmisku kiberincidentu Eiropas līmeņa koordinācijas mehānisma (EU-SCICF) izveide

Attiecībā uz A ieteikuma 1. punktu tiek noteikti šādi atbilstības kritēriji:

1. Gatavojoties efektīvai Savienības līmeņa koordinētai reakcijai, kurai būtu jāietver pakāpeniska EU-SCICF attīstība, īstenojot pilnvaras, kas paredzētas gaidāmajā Eiropas Parlamenta un Padomes Regulā par finanšu sektora digitālās darbības noturību (turpmāk – "DORA"), Eiropas uzraudzības iestādēm (EUI), kas rīkojas ar Apvienotās komitejas starpniecību un kopā ar Eiropas Centrālo banku (ECB), Eiropas Sistēmisko risku kolēģiju (ESRK) un attiecīgajām nacionālajām iestādēm, un vajadzības gadījumā apspriežoties ar Eiropas Savienības Tīklu un informācijas drošības aģentūru un Komisiju, būtu jāapsver vismaz šādu aspektu iekļaušana paredzētajā EU-SCICF sagatavošanā:

   a. EU-SCICF efektīvai attīstībai vajadzīgo resursu analīze;

   b. krīzes pārvarēšanas un ārkārtas mācību izstrāde, ietverot kiberuzbrukumu scenārijus, lai attīstītu saziņas kanālus;

   c. kopējas vārdnīcas izstrāde;

   d. saskaņotas kiberincidentu klasifikācijas izstrāde;

   e. drošu un uzticamu informācijas apmaiņas kanālu, tostarp dublēšanas sistēmu, izveide;

   f. kontaktpunktu izveide;

   g. konfidencialitātes informācijas apmaiņā risinājumi;

   h. sadarbības un informācijas apmaiņas ar finanšu nozares kiberizlūkošanu iniciatīvas;

   i. efektīvu aktivizēšanas un eskalācijas procesu izstrāde, izmantojot situācijas apzināšanos;

   j. sistēmas dalībnieku pienākumu precizēšana;

   k. saskarņu izstrāde starpnozaru un attiecīgā gadījumā trešo valstu koordinācijai;

   l. attiecīgo iestāžu saskaņotas saziņas ar sabiedrību nodrošināšana, lai saglabātu uzticēšanos;

   m. iepriekš noteiktu komunikācijas līniju izveide savlaicīgai saziņai;

   n. atbilstošu pamattestēšanas pasākumu, tostarp starpjurisdikciju testēšanas un trešo valstu koordinācijas, un novērtējumu, kuru rezultātā tiek gūta pieredze un sistēmas attīstība, veikšana;

   o. efektīvas saziņas un dezinformācijas pretpasākumu nodrošināšana.

B ieteikums. EU-SCICF kontaktpunktu izveide

Attiecībā uz B ieteikumu tiek noteikti šādi atbilstības kritēriji:

1. EUI, ECB un katrai dalībvalstij, izvēloties kādu no savām attiecīgajām nacionālajām iestādēm, būtu jāvienojas par vienotu pieeju attiecībā uz EU-SCICF norīkoto kontaktpunktu saraksta kopīgošanu un atjaunināšanu.

2. Kontaktpunkta norīkošana būtu jānovērtē, ņemot vērā vienoto kontaktpunktu saskaņā ar Direktīvu (ES) 2016/1148, ko dalībvalstis izveidojušas attiecībā uz tīklu un informācijas sistēmu drošību, lai nodrošinātu pārrobežu sadarbību ar citām dalībvalstīm un Tīklu un informācijas sistēmu sadarbības grupu.

C ieteikums. Izmaiņas Savienības tiesiskajā regulējumā

Attiecībā uz C ieteikumu tiek noteikti šādi atbilstības kritēriji:

Komisijai būtu jāapsver, vai analīzes, kas veikta saskaņā ar A ieteikumu, rezultātā vajadzīgi kādi pasākumi, tostarp izmaiņas attiecīgajos Savienības tiesību aktos, lai nodrošinātu, ka EUI ar Apvienotās komitejas starpniecību un kopā ar ECB, ESRK un attiecīgajām nacionālajām iestādēm var izstrādāt EU-SCICF saskaņā ar A ieteikuma 1. punktu, un lai nodrošinātu, ka EUI, ECB, ESRK un attiecīgās nacionālās iestādes, kā arī citas iestādes var iesaistīties koordinācijas darbībās un informācijas apmaiņā, kas ir pietiekami detalizēta un konsekventa, lai atbalstītu efektīvu EU-SCICF darbību.