I

(Resolutsioonid, soovitused ja arvamused)

SOOVITUSED

EUROOPA SÜSTEEMSETE RISKIDE NÕUKOGU

EUROOPA SÜSTEEMSETE RISKIDE NÕUKOGU SOOVITUS,

2. detsember 2021,

seoses üleeuroopalise süsteemsete küberintsidentide koordineerimisraamistikuga asjaomastele asutustele

(ESRN/2021/17)

(2022/C 134/01)

EUROOPA SÜSTEEMSETE RISKIDE NÕUKOGU HALDUSNÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Majanduspiirkonna lepingut ([1]), eelkõige selle IX lisa,

võttes arvesse Euroopa Parlamendi ja nõukogu määrust (EL) nr 1092/2010, 24. november 2010, finantssüsteemi makrotasandi usaldatavusjärelevalve kohta Euroopa Liidus ja Euroopa Süsteemsete Riskide Nõukogu asutamise kohta ([2]), eelkõige selle artikli 3 lõike 2 punkte b ja d ning artikleid 16 ja 18,

võttes arvesse Euroopa Süsteemsete Riskide Nõukogu otsust ESRN/2011/1, 20. jaanuar 2011, millega võetakse vastu Euroopa Süsteemsete Riskide Nõukogu töökord ([3]), eelkõige selle artikleid 18 kuni 20,

ning arvestades järgmist:

(1) Euroopa Süsteemsete Riskide Nõukogu soovituse ESRN/2013/1 ([4]) põhjenduse 4 kohaselt on makrotasandi usaldatavusjärelevalve poliitika lõppeesmärk finantssüsteemi kui terviku stabiilsuse tagamisele kaasa aitamine finantssüsteemi vastupanuvõime suurendamise ja süsteemsete riskide kuhjumise vähendamise kaudu, mis tagab finantssektori jätkusuutliku panuse majanduskasvu. Euroopa Süsteemsete Riskide Nõukogu (ESRN) vastutab makrotasandi finantsjärelevalve teostamise eest liidus. Oma pädevuse täitmiseks peab ESRN kaasa aitama finantsstabiilsuse süsteemsete riskide, sh küberintsidentidega seotud riskide, ärahoidmisele ja leevendamisele ning tegema ettepanekuid asjaomaste riskide maandamiseks.

(2) Kuna olulised küberintsidendid võivad kahjustada kriitilise tähtsusega finantsteenuseid ja -operatsioone, võivad nad põhjustada süsteemset riski finantssüsteemis. Esialgne šokk võib võimenduda läbi äritegevusega seotud negatiivse mõju või finantsstressi ülekandumise, samuti läbi usalduse õõnestamise finantssüsteemi vastu. Kui finantssüsteem ei suuda sellistele šokkidele vastu seista, seab see ohtu finantsstabiilsuse ning võib põhjustada süsteemse küberkriisi ([5]).

([1]) EÜT L 1, 3.1.1994, lk 3.
([2]) ELT L 331, 15.12.2010, lk 1.
([3]) ELT C 58, 24.2.2011, lk 4.
([4]) Euroopa Süsteemsete Riskide Nõukogu soovitus ESRN/2013/1, 4. aprill 2013, vahe-eesmärkide ja makrotasandi usaldatavusjärelevalve poliitika instrumentide kohta (ELT C 170, 15.6.2013, lk 1).
([5]) Vt „Systemic cyber risk“, ESRN, veebruar 2020, avaldatud ESRNi veebilehel www.esrb.europa.eu

(3) Pidevalt muutuv küberohtude maastik ja oluliste küberintsidentide arvu kasv näitab, et risk liidu finantsstabiilsusele on suurenenud. COVID-19 pandeemia on näidanud, kui olulist rolli mängib tehnoloogia finantssüsteemi toimimisel. Kaugtöö vajaduse suurenemise tõttu pidid kõik asjaomased asutused oma tehnilist taristut ja riskiohjeraamistikku kohandama, mis on omakorda suurendanud finantssüsteemi küberriske ning andnud kurjategijatele võimaluse rakendada uusi ja täiendada varem kasutatud meetodeid olukorra enda huvides ära kasutamiseks ([6]). EKP pangandusjärelevalve andmetel on küberintsidentide arv 2020. aastal kasvanud 54 %, võrreldes 2019. aastaga ([7]).

(4) Olulise küberintsidendi potentsiaalselt laiaulatusliku mõju ning levimise kiiruse ja ulatuse tõttu on asjaomastel asutustel vaja tõhusalt reageerida, et leevendada võimalikku negatiivset mõju finantsstabiilsusele. Asjaomaste asutuste vaheline sujuv koostöö ja teabevahetus liidu tasandil aitab varakult hinnata olulise küberintsidendi mõju finantsstabiilsusele, säilitada usaldust finantssüsteemi vastu ning piirata teiste finantseerimisasutuste nakatamise ohtu, aidates vältida küberintsidendist põhjustatud riski finantsstabiilsusele.

(5) Algne šokk tekib teistmoodi kui traditsiooniline finants- ja likviidsuskriis, millega asjaomased asutused tavapäraselt kokku puutuvad. Lisaks finantsküsimustele peab riskihinnang hõlmama ka äritegevuse katkestuste ulatust ja mõju, kuna need võivad mõjutada makrotasandi usaldatavusjärelevalve vahendite valikut. Samuti võib finantsstabiilsus mõjutada äritegevuse riske maandavate tegurite valikut küberekspertide poolt. Selleks on vaja tihedat ja sujuvat koostööd ning avatud suhtlemist, et muu hulgas suurendada olukorrateadlikkust.

(6) Riski, et asutuste töö koordineerimine võib olla puudulik, tuleb teadvustada ja seda maandada. Liidu asjaomased asutused peavad tööd koordineerima nii omavahel kui muude asutustega, kellega nad tavapäraselt kokku ei puutu, nt Euroopa Liidu Küberturvalisuse Ametiga (ENISA). Kuna märkimisväärne arv liidu finantseerimisasutusi tegutseb globaalsel tasandil, ei pruugi võimalik oluline küberintsident olla piiratud liidu territooriumiga ning võib algselt tekkida väljaspool liitu, ning vajab globaalset koordineerimist.

(7) Asjaomased asutused peavad olema selliseks koostööks valmis. Vastasel juhul võib vastuoluline tegevus kahjustada teiste asutuste reageerimistegevust. Tegevuse kooskõlastamata jätmine võib finantssüsteemi šokki võimendada ning õõnestada usaldust finantssüsteemi toimimise vastu, mis võib halvimal juhul ohustada finantsstabiilsust ([8]). Seetõttu tuleb astuda vajalikke samme, et käsitleda riske, mida olulise küberintsidendiga seotud tegevuse kooskõlastamata jätmine võib finantssüsteemis tekitada.

(8) ESRNi (2021) aruandes *Mitigating systemic cyber risk* ([9]) peetakse vajalikuks kehtestada üleeuroopaline süsteemsete küberintsidentide koordineerimisraamistik (EU-SCICF) liidu asjaomastele asutustele. EU-SCICFi eesmärk oleks suurendada asjaomaste asutuste valmisolekut koordineeritult reageerida võimalikele olulistele küberintsidentidele. ESRNi (2021) aruandes *Mitigating systemic cyber risk* on välja toodud ESRNi esialgne hinnang selle kohta, millised omadused asjaomasel raamistikul peaksid olema, et vältida tegevuse kooskõlastamata jätmisega seonduvaid riske.

(9) Käesoleva soovituse põhieesmärk on suurendada kavandatava Euroopa Parlamendi ja nõukogu määrusega, mis käsitleb finantssektori digitaalset tegevuskerksust ([10]) (edaspidi „DORA määrus“), Euroopa järelevalveasutustele ette nähtud rolli, et järk-järgult tõhustada liidu tasandil koordineeritud reageerimist piiriülestele info- ja kommunikatsioonitehnoloogiaga (IKTga) seotud olulistele intsidentidele või nendega seotud ohtudele, millel on süsteemne mõju kogu liidu finantssektorile. Selle protsessi tulemusena luuakse EU-SCICF asjaomastele asutustele.

([6]) Vt „Internet Organised Crime Threat Assessment“, Europol, 2020, avaldatud Europoli veebilehel www.europol.europa.eu
([7]) Vt „IT and cyber risk: a constant challenge“, EKP, 2021, avaldatud EKP pangandusjärelevalve veebilehel www.bankingsupervision.europa.eu
([8]) Vt „Systemic cyber risk“, ESRN, veebruar 2020, avaldatud ESRNi veebilehel www.esrb.europa.eu
([9]) Vt „Mitigating systemic cyber risk“, ESRN 2021 (avaldatakse varsti).
([10]) COM/2020/595 final.

(10) EU-SCICFi eesmärk ei ole asendada olemasolevaid raamistikke, vaid täita võimalikud lüngad tegevuse kooskõlastamisel ja teabe vahetamisel asjaomaste asutuste vahel ning teiste liidu asutuste ja oluliste partneritega rahvusvahelisel tasandil. Sellega seoses tuleb kaaluda EU-SCICFi positsiooni olemasolevas finantskriisiraamistikus ning liidu küberintsidentide raamistikus. Asjaomaste asutuste vahelise tegevuse kooskõlastamise osas peab muu hulgas arvestama finantssektori ettevõtjate jaoks Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148 ([11]) alusel moodustatud võrgu- ja infoturbe koostöörühma ning ENISA kaasabil loodava ühise küberüksuse koordineerimismehhanisme.

(11) Eelkõige on EU-SCICFi moodustamise alustamise ettepaneku eesmärk toetada kavandatavas DORAs ette nähtud Euroopa järelevalveasutuste võimalikku rolli. Olukorrateadlikkuse suurendamiseks ning sektorite ühiste küberhaavatavuste ja -ohtude kindlaks tegemiseks näeb DORA määrus ette, et Euroopa järelevalveasutused võivad „ühiskomitee kaudu ning koostöös pädevate asutuste, Euroopa Keskpanga (EKP) ja ESRNiga luua mehhanisme, mis võimaldavad jagada finantssektorite vahel tõhusaid tavasid“ ning „välja töötada kriisijuhtimis- ja erandolukorra simulatsioone, mis hõlmavad küberrünnete stsenaariume, et töötada välja sidekanalid ja võimaldada järk-järgult tõhusat koordineeritud reageerimist ELi tasandil IKTga seotud olulise piiriülese intsidendi või seonduva ohu korral, millel on süsteemne mõju liidu finantssektorile tervikuna“ ([12]). EU-SCICFi sarnast üleeuroopalist raamistikku ei ole veel loodud, ning see tuleks DORA määruse alusel luua ja välja arendada.

(12) Võttes arvesse küberohust tulenevat riski liidu finantsstabiilsusele tuleks ettevalmistustöid EU-SCICFi loomiseks võimalikult suures ulatuses alustada juba enne seda, kui selle loomiseks vajalik õigus- ja poliitikaraamistik on täielikult kohaldatud. Õigus- ja poliitikaraamistik kujundatakse ja viimistletakse pärast seda, kui DORA määruse ja sellega seotud delegeeritud õigusaktide asjaomased sätted on kohaldatud.

(13) Tulemuslik teabevahetus aitab suurendada asjaomaste asutuste olukorrateadlikkust ning on seetõttu hädavajalik eeltingimus oluliste küberintsidentidega seotud tegevuste liiduülese koordineerimise tagamiseks. Seetõttu tuleb kindlaks määrata olulisele küberintsidendile reageerimise koordineerimiseks vajalik sidetaristu. Selleks tuleb täpsustada, millist liiki teavet jagatakse, milliseid kanaleid selleks tavapäraselt kasutatakse ning milliste kontaktpunktidega teavet jagatakse. Teabe jagamisel tuleb järgida kehtestatud õigusnorme. Lisaks võib asjaomastel asutustel olla vaja kehtestada konkreetne tegevuskava ja protokollid, mida tuleb järgida, et tagada nõuetekohane kooskõlastamine asutustega, kes on kaasatud koordineeritud reageerimisse olulisele küberintsidendile.

(14) Süsteemse küberkriisi korral on vaja teha täielikku koostööd nii riikide kui liidu tasandil. Seetõttu võib olla vaja määrata Euroopa järelevalveasutustele, EKP-le ja igale liikmesriigile asjaomaste riigi ametiasutuste hulgast kontaktpunktid, mis tuleb edastada Euroopa järelevalveasutustele, et määratleda EU-SCICFi koordineerimisskeemi peamised koostööpartnerid, keda olulisest küberintsidendist teavitada. Kontaktpunktide määramise vajadust tuleb hinnata EU-SCICFi välja töötamisel, võttes arvesse direktiivi (EL) 2016/1148 kohaselt määratud ühtseid kontaktpunkte, mille liikmesriigid on nimetanud võrgu- ja infosüsteemide turvalisuse huvides selleks, et tagada piiriülene koostöö teiste liikmesriikide ning võrgu- ja infoturbe koostöörühmaga ([13]).

(15) Kriisijuhtimis- ja erandolukorra simulatsioonid aitavad kaasa EU-SCICFi rakendamisele ning võimaldavad asjaomastel asutustel hinnata oma valmisolekut ja ettevalmistust võimalikuks süsteemseks küberkriisiks liidu tasandil. Sellised simulatsioonid on asjaomaste asutuste jaoks võimalus õppida ning EU-SCICIFi pidevalt täiustada ja arendada.

([11]) Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/1148, 6. Juuli 2016, meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.7.2016, lk 1).

([12]) Vt kavandatava DORA määruse artikkel 43.

([13]) Vt Euroopa Komisjon, „NIS Cooperation Group“, avaldatud komisjoni veebilehel www.ec.europa.eu

(16) EU-SCICFi välja töötamiseks on oluline, et Euroopa järelevalveasutused teeksid ühiselt ettevalmistusi raamistiku võimalike oluliste elementide, vajalike ressursside ning arenguvajaduste läbi töötamiseks. Pärast seda saavad Euroopa järelevalveasutused alustada esialgse analüüsi läbiviimist võimalike takistuste osas, millega Euroopa järelevalveasutused ja asjaomased asutused võivad EU-SCICFi loomisel ja vajaliku teabe sidekanalite kaudu jagamisel olulise küberintsidendi korral kokku puutuda. See analüüs on oluline etapp, mis annab sisendi mis tahes edasistele sammudele nii õigusloome kui muude tugitegevuste osas, mida Euroopa Komisjon võib algatada pärast DORA määruse rakendamist.

ON VASTU VÕTNUD KÄESOLEVA SOOVITUSE:

1. JAGU

SOOVITUSED

Soovitus A – Üleeuroopalise süsteemsete küberintsidentide koordineerimisraamistiku (EU-SCICF) loomine

1. Nagu on ette nähtud komisjoni ettepanekus Euroopa Parlamendi ja nõukogu määruse kohta, mis käsitleb finantssektori digitaalset tegevuskerksust (edaspidi „DORA“ määrus), soovitatakse Euroopa järelevalveasutustel oma ühiskomitee kaudu ning koos Euroopa Keskpanga (EKP), Euroopa Süsteemsete Riskide Nõukogu (ESRN) ja asjaomaste riigi ametiasutustega alustada ettevalmistusi tulemusliku liidu tasandil koordineeritud reageerimise järk-järguliseks välja arendamiseks sellise piiriülese olulise küberintsidendi või -ohu tõrjumiseks, millel võib olla süsteemne mõju liidu finantssektorile. Ettevalmistused liidu tasandil koordineeritud reageerimiseks peaksid hõlmama EU-SCICFI järk-järgulist välja töötamist Euroopa järelevalveasutuse, EKP, ESRNi ja asjaomaste riigi ametiasutuste jaoks. Samuti peaks ettevalmistused hõlmama EU-SCICFi tulemuslikuks välja töötamiseks vajalike ressursside hindamist.

2. Euroopa järelevalveasutustel soovitatakse soovituse A punkti 1 osas alustada konsultatsioone EKP ja ESRNiga, et kaardistada ning seejärel analüüsida võimalikke õiguslikke või menetluslikke takistusi EU-SCICFi tulemuslikuks välja töötamiseks.

Soovitus B – EU-SCICFi konktaktpunktide määramine

Euroopa järelevalveasutustel, EKP-l ja igal liikmesriigil soovitatakse oma asjaomaste riigi ametiasutuste hulgast määrata peamine kontaktpunkt, ning sellest teavitada Euroopa järelevalveasutusi. Kontaktide nimekiri aitab kaasa raamistiku arendamisele ning kui EU-SCICF on loodud, tuleb neid kontaktpunkte ja ESRNi olulisest küberintsidendist teavitada. Samuti tuleb ette näha töö koordineerimine EU-SCICFi ja direktiiviga (EL) 2016/1148 kindlaks määratud ühtsete kontaktpunktide vahel, mille liikmesriigid on nimetanud võrgu- ja infosüsteemide turvalisuse huvides selleks, et tagada piiriülene koostöö teiste liikmesriikide ning võrgu- ja infoturbe koostöörühmaga.

Soovitus C – asjakohased meetmed liidu tasandil

Komisjonil soovitatakse soovituse A kohaselt läbi viidud analüüsi tulemuste põhjal kaaluda, millised asjakohased meetmed aitaksid tagada tulemusliku süsteemsetele küberintsidentidele reageerimise koordineerimise.

2. JAGU

RAKENDAMINE

1. **Mõisted**

Käesolevas soovituses kasutatakse mõisteid järgmises tähenduses:

a) „küber-“ (*cyber*) - inimeste, protsesside, andmete ja infosüsteemide vaheliste vastasmõjude ühendatud infotaristuga seotult, selle taristu siseselt või selle taristu abil ([14]);

([14]) Vt „Cyber Lexicon“, finantsstabiilsuse nõukogu, 12. november 2018, avaldatud finantsstabiilsuse nõukogu veebilehel www.fsb.org

b) „oluline küberintsident“ (*major cyber incident*) - IKTga seotud oluline intsident, millel võib olla suur negatiivne mõju võrgu- ja infosüsteemidele, mis toetavad finantssektori ettevõtja kriitilise tähtsusega funktsioone ([15]);

c) „süsteemne küberkriis“ (*systemic cyber crisis*) - oluline küberintsident, mis põhjustab liidu finantssüsteemis selliseid häiringuid, millel võivad olla tõsised negatiivsed tagajärjed siseturu tõrgeteta toimimisele ja reaalmajanduse toimimisele. Selline kriis võib tekkida olulise küberintsidendi tagajärjel, mis põhjustab šokke erinevates kanalites, sh seoses äritegevuse, usalduse või rahaliste vahenditega.

d) „Euroopa järelevalveasutused“ (*European Supervisory Authorities*, ESAs) - Euroopa Parlamendi ja nõukogu määrusega (EL) nr 1093/2010 ([16]) asutatud Euroopa Järelevalveasutus (Euroopa Pangandusjärelevalve) koos Euroopa Parlamendi ja nõukogu määrusega (EL) nr 1094/2010 ([17]) asutatud Euroopa Järelevalveasutuse (Euroopa Kindlustus- ja Tööandjapensionide Järelevalve) ja Euroopa Parlamendi ja nõukogu määrusega (EL) nr 1095/2010 ([18]) asutatud Euroopa Järelevalveasutusega (Euroopa Väärtpaberiturujärelevalve);

e) „ühiskomitee“ (*Joint Committee)* - määruse (EL) nr 1093/2010, määruse (EL) nr 1094/2010 ja määruse (EL) nr 1095/2010 artiklis 54 ette nähtud Euroopa järelevalveasutuste ühiskomitee;

f) „asjaomane riigi ametiasutus“ (*relevant national authority*) –

1. määruse (EL) nr 1093/2010, määruse (EL) nr 1094/2010 ja määruse (EL) nr 1095/2010 artikli 1 lõikes 2 osutatud liidu õigusaktides määratletud liikmesriikide pädev asutus või järelevalveasutus ning muu riiklik pädev asutus, mis on määratletud liidu õigusaktides, millega antakse ülesandeid Euroopa järelevalveasutustele;

2. liikmesriigi pädev asutus, kes on määratud järgmiste normide alusel:

i. Euroopa Parlamendi ja nõukogu direktiivi 2013/36/EL artikkel 4 ([19]), ilma et see piiraks EKP-le nõukogu määrusega (EL) nr 1024/2013 antud eriülesandeid ([20]);

ii. Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/2366 ([21]) artikkel 22;

iii. Euroopa Parlamendi ja nõukogu direktiivi 2009/110/EÜ ([22]) artikkel 37;

iv. Euroopa Parlamendi ja nõukogu direktiivi (EL) 2019/2034 ([23]) artikkel 4;

([15]) Vt ettepandud DORA määruse artikli 3 punkt 7.

([16]) Euroopa Parlamendi ja nõukogu määrus (EL) nr 1093/2010, 24. november 2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Pangandusjärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/78/EÜ (ELT L 331, 15.12.2010, lk 12).

([17]) Euroopa Parlamendi ja nõukogu määrus (EL) nr 1094/2010, 24. november 2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Kindlustus- ja Tööandjapensionide Järelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/79/EÜ (ELT L 331, 15.12.2010, lk 48).

([18]) Euroopa Parlamendi ja nõukogu määrus (EL) nr 1095/2010, 24. november 2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Väärtpaberiturujärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/77/EÜ (ELT L 331, 15.12.2010, lk 84).

([19]) Euroopa Parlamendi ja nõukogu direktiiv 2013/36/EL, 26. juuni 2013, mis käsitleb krediidiasutuste tegevuse alustamise tingimusi ning krediidiasutuste usaldatavusnõuete täitmise järelevalvet, millega muudetakse direktiivi 2002/87/EÜ ning millega tunnistatakse kehtetuks direktiivid 2006/48/EÜ ja 2006/49/EÜ (ELT L 176, 27.6.2013, lk 338).

([20]) Nõukogu määrus (EL) nr 1024/2013, 15. oktoober 2013, millega antakse Euroopa Keskpangale eriülesanded seoses krediidiasutuste usaldatavusnõuete täitmise järelevalve poliitikaga (ELT L 287, 29.10.2013, lk 63).

([21]) Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/2366, 25. november 2015, makseteenuste kohta siseturul, direktiivide 2002/65/EÜ, 2009/110/EÜ ning 2013/36/EL ja määruse (EL) nr 1093/2010 muutmise ning direktiivi 2007/64/EÜ kehtetuks tunnistamise kohta (ELT L 337, 23.12.2015, lk 35).

([22]) Euroopa Parlamendi ja nõukogu direktiiv 2009/110/EÜ, 16. september 2009, mis käsitleb e-raha asutuste asutamist ja tegevust ning usaldatavusnormatiivide täitmise järelevalvet ning millega muudetakse direktiive 2005/60/EÜ ja 2006/48/EÜ ning tunnistatakse kehtetuks direktiiv 2000/46/EÜ (ELT L 267, 10.10.2009, lk 7).

([23]) Euroopa Parlamendi ja nõukogu direktiiv 2019/2034, 27. november 2019, mis käsitleb investeerimisühingute usaldatavusnõuete täitmise järelevalvet ning millega muudetakse direktiive 2002/87/EÜ, 2009/65/EÜ, 2011/61/EL, 2013/36/EL, 2014/59/EL ja 2014/65/EL (ELT L 314, 5.12.2019, lk 64).

v. ettepanek võtta vastu Euroopa Parlamendi ja nõukogu määrus, mis käsitleb krüptovararturge ja millega muudetakse direktiivi (EL) 2019/1937 ([24]), artikli 3 lõike 1 punkti ee esimene taane;

vi. Euroopa Parlamendi ja nõukogu määruse (EL) nr 909/2014 ([25]) artikkel 11;

vii. Euroopa Parlamendi ja nõukogu määruse (EL) nr 648/2012 ([26]) artikkel 22;

viii. Euroopa Parlamendi ja nõukogu direktiivi 2014/65/EL ([27]) artikkel 67;

ix. määruse (EL) nr 648/2012 artikkel 22;

x. Euroopa Parlamendi ja nõukogu direktiivi 2011/61/EL ([28]) artikkel 44;

xi. Euroopa Parlamendi ja nõukogu direktiivi 2009/65/EL ([29]) artikkel 97;

xii. Euroopa Parlamendi ja nõukogu direktiivi 2009/138/EL ([30]) artikkel 30;

xiii. Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/97 ([31]) artikkel 12;

xiv. Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/2341 ([32]) artikkel 47;

xv. Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 1060/2009 ([33]) artikkel 22;

xvi. Euroopa Parlamendi ja nõukogu direktiivi 2006/43/EL ([34]) artikli 3 lõige 2 ja artikkel 32;

xvii. Euroopa Parlamendi ja nõukogu määruse (EL) nr 2016/1011 ([35]) artikkel 40;

xviii. Euroopa Parlamendi ja nõukogu määruse (EL) nr 2020/1503 ([36]) artikkel 29;

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

([25]) Euroopa Parlamendi ja nõukogu määrus (EL) nr 909/2014, 23. juuli 2014, mis käsitleb väärtpaberiarvelduse parandamist Euroopa Liidus ja väärtpaberite keskdepositooriume ning millega muudetakse direktiive 98/26/EÜ ja 2014/65/EL ning määrust (EL) nr 236/2012 (ELT L 257, 28.8.2014, lk 1).

([26]) Euroopa Parlamendi ja nõukogu määrus (EL) nr 648/2012, 4. juuli 2012, börsiväliste tuletisinstrumentide, kesksete vastaspoolte ja kauplemisteabehoidlate kohta (ELT L 201, 27.7.2012, lk 1).

([27]) Euroopa Parlamendi ja nõukogu direktiiv 2014/65/EL, 15. mai 2014, finantsinstrumentide turgude kohta ning millega muudetakse direktiive 2002/92/EÜ ja 2011/61/EL (ELT L 173, 12.6.2014, lk 349).

([28]) Euroopa Parlamendi ja nõukogu direktiiv 2011/61/EL, 8. juuni 2011, alternatiivsete investeerimisfondide valitsejate kohta, millega muudetakse direktiive 2003/41/EÜ ja 2009/65/EÜ ning määruseid (EÜ) nr 1060/2009 ja (EL) nr 1095/2010 (ELT L 174, 1.7.2011, lk 1).

([29]) Euroopa Parlamendi ja nõukogu direktiiv 2009/65/EÜ, 13. juuli 2009, vabalt võõrandatavatesse väärtpaberitesse ühiseks investeeringuks loodud ettevõtjaid (eurofondid) käsitlevate õigus- ja haldusnormide kooskõlastamise kohta (ELT L 302, 17.11.2009, lk 32).

([30]) Euroopa Parlamendi ja nõukogu direktiiv 2009/138/EÜ, 25. november 2009, kindlustus- ja edasikindlustustegevuse alustamise ja jätkamise kohta (Solventsus II) (ELT L 335, 17.12.2009, lk 1).

([31]) Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/97, 20. jaanuar 2016, mis käsitleb kindlustustoodete turustamist (ELT L 26, 2.2.2016, lk 19).

([32]) Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/2341, 14. detsember 2016, tööandja kogumispensioni asutuste tegevuse ja järelevalve kohta (ELT L 354, 23.12.2016, lk 37).

([33]) Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1060/2009, 16. september 2009, reitinguagentuuride kohta, (ELT L 302, 17.11.2009, lk 1).

([34]) Euroopa Parlamendi ja nõukogu direktiiv 2006/43/EÜ, 17. mai 2006, mis käsitleb raamatupidamise aastaaruannete ja konsolideeritud aruannete kohustuslikku auditit ning millega muudetakse nõukogu direktiive 78/660/EMÜ ja 83/349/EMÜ ning tunnistatakse kehtetuks nõukogu direktiiv 84/253/EMÜ (ELT L 157, 9.6.2006, lk 87).

([35]) Euroopa Parlamendi ja nõukogu määrus (EL) 2016/1011, 8. juuni 2016, mis käsitleb indekseid, mida kasutatakse võrdlusalustena finantsinstrumentide ja -lepingute puhul või investeerimisfondide tootluse mõõtmiseks, ning millega muudetakse direktiive 2008/48/EÜ ja 2014/17/EL ning määrust (EL) nr 596/2014 (ELT L 171, 29.6.2016, lk 1).

([36]) Euroopa Parlamendi ja nõukogu määrus (EL) 2020/1503, 7. oktoober 2020, mis käsitleb ettevõtjatele Euroopa ühisrahastusteenuse osutajaid ning millega muudetakse määrust (EL) 2017/1129 ja direktiivi (EL) 2019/1937 (ELT L 347, 20.10.2020, lk 1).

3. Järgmised ametiasutused, kelle ülesandeks on makrotasandi usaldatavusjärelevalve meetmete vastuvõtmine ja/või käivitamine või muud finantsstabiilsuse ülesanded, näiteks seoses põhjendava analüüsiga (mittetäielik loetelu):

   i. määratud asutus direktiivi 2013/36/EL VII jaotise 4. peatüki või Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013 ([37]) artikli 458 lõike 1 kohaselt;

   ii. makrotasandi usaldatavusjärelevalve asutus, kelle eesmärk, institutsionaalne korraldus, ülesanded, volitused, vahendid, aruandekohustus jms on määratletud Euroopa Süsteemsete Riskide Nõukogu soovituses ESRN/2011/3 ([38]).

g) „asjaomane asutus“ (*relevant authority*) –

   1. Euroopa järelevalveasutus;

   2. EKP talle määruse (EL) nr 1024/2013 artikli 4 lõigetega 1 ja 2 ning artikli 5 lõikega 2 antud ülesannete osas;

   3. asjaomane riigi ametiasutus.

2. **Rakendamise kriteeriumid**

Käesoleva soovituse rakendamisel kohaldatakse järgmisi kriteeriume:

a) kohast tähelepanu tuleb pöörata teadmisvajaduse ja proportsionaalsuse põhimõttele, võttes arvesse iga soovituse eesmärki ja sisu;

b) lisas sätestatud konkreetsed vastavuskriteeriumid peavad olema täidetud iga soovituse suhtes.

3. **Edasine ajakava**

Määruse (EL) nr 1092/2010 artikli 17 lõike 1 kohaselt peavad adressaadid teavitama Euroopa Parlamenti, nõukogu, komisjoni ja ESRNi meetmetest, mis on võetud käesoleva soovituse rakendamiseks, või põhjendama meetmete võtmata jätmist. Adressaadid peavad nimetatud teavituse esitama järgmisteks tähtaegadeks:

1. Soovitus A

   a) Euroopa järelevalveasutused peavad Euroopa Parlamendile, nõukogule, komisjonile ja ESRNile esitama soovituse A punkti 1 rakendamise vahearuande 30. juuniks 2023, kuid mitte varem kui 6 kuud pärast DORA määruse jõustumist.

   b) Euroopa järelevalveasutused peavad Euroopa Parlamendile, nõukogule, komisjonile ja ESRNile esitama soovituse A punkti 1 rakendamise lõpparuande 30. juuniks 2024, kuid mitte varem kui 18 kuud pärast DORA määruse jõustumist.

   c) Euroopa järelevalveasutused peavad Euroopa Parlamendile, nõukogule, komisjonile ja ESRNile esitama soovituse A punkti 2 rakendamise aruande 30. juuniks 2025, kuid mitte varem kui 30 kuud pärast DORA määruse jõustumist.

2. Soovitus B

   Euroopa järelevalveasutused, EKP ja liikmesriigid peavad Euroopa Parlamendile, nõukogule, komisjonile ja ESRNile esitama soovituse B rakendamise aruande 30. juuniks 2023, kuid mitte varem kui kuus kuud pärast DORA määruse jõustumist.

3. Soovitus C

   a) Komisjon peab Euroopa Parlamendile, nõukogule ja ESRNile esitama soovituse C rakendamise aruande 31. detsembriks 2023, kuid mitte varem kui 12 kuud pärast DORA määruse jõustumist, võttes arvesse Euroopa järelevalveasutuste poolt kooskõlas soovituse A punktiga 1 esitatud vahearuannet.

([37]) Euroopa Parlamendi ja nõukogu määrus (EL) nr 575/2013, 26. juuni 2013, krediidiasutuste ja investeerimisühingute suhtes kohaldatavate usaldatavusnõuete kohta ja määruse (EL) nr 648/2012 muutmise kohta (ELT L 176, 27.6.2013, lk 1).

([38]) Euroopa Süsteemsete Riskide Nõukogu soovitus ESRN/2011/3, 22. detsember 2011, riigi ametiasutuste makrotasandi usaldatavusjärelevalve pädevuse kohta (ELT C 41, 14.2.2012, lk 1).

b) Komisjon peab Euroopa Parlamendile, nõukogule ja ESRNile esitama soovituse C rakendamise aruande 31. detsembriks 2025, kuid mitte varem kui 36 kuud pärast DORA määruse jõustumist, võttes arvesse Euroopa järelevalveasutuste poolt kooskõlas soovitusega A esitatavaid aruandeid.

4. **Jälgimine ja hindamine**

1. ESRNi sekretariaat:

a) abistab adressaate, tagab aruandluse kooskõlastamise ja asjakohaste vormide koostamise ning täpsustab vajadusel meetmete võtmise korda ja tähtaegu;

b) kontrollib järelmeetmete järgimist adressaatide poolt, abistab neid vajaduse korral ning esitab haldusnõukogule järelmeetmete aruande. Hinnangud antakse järgmiselt:

i) soovituste A ja B rakendamise kohta 12 kuu jooksul pärast DORA määruse jõustumist;

ii) soovituse C rakendamise kohta 18 kuu jooksul pärast DORA määruse jõustumist;

iii) soovituse A rakendamise kohta 24 kuu jooksul pärast DORA määruse jõustumist;

iv) soovituse A rakendamise kohta 36 kuu jooksul pärast DORA määruse jõustumist;

v) soovituse C rakendamise kohta 42 kuu jooksul pärast DORA määruse jõustumist.

2. Haldusnõukogu hindab adressaatide meetmeid ja põhjendusi ning võib asjakohastel juhtudel otsustada, et käesolevat soovitust ei ole järgitud ning et adressaadi põhjendused tegevusetuse kohta ei ole piisavad.

Frankfurt Maini ääres, 2. detsember 2021

ESRNi haldusnõukogu nimel
ESRNi sekretariaadi juhataja
Francesco MAZZAFERRO

LISA

SOOVITUSE SUHTES KOHALDATAVAD VASTVUSKRITEERIUMID

Soovitus A – Üleeuroopalise süsteemsete küberintsidentide koordineerimisraamistiku (EU-SCICF) loomine

Soovituse A punkti 1 osas kehtivad järgmised vastavuskriteeriumid.

1. Selleks, et teha ettevalmistusi tulemusliku liidu tasandil koordineeritud reageerimisvõime välja arendamiseks, mis hõlmaks EU-SCICFi järk-järgulist välja arendamist volituste abil, mis nähakse ette kavandatava Euroopa Parlamendi ja nõukogu määrusega, mis käsitleb finantssektori digitaalset tegevuskerksust (edaspidi „DORA määrus"), peavad Euroopa järelevalveasutused oma ühiskomitee kaudu ning koos Euroopa Keskpanga (EKP), Euroopa Süsteemsete Riskide Nõukogu (ESRN) ja asjaomaste riigi ametiasutustega, asjakohastel juhtudel pärast Euroopa Liidu Küberturvalisuse Ameti ja komisjoniga konsulteerimist, kaaluma vähemalt järgmiste tegevuste lisamist EU-SCICF ettevalmistustesse:

   a. EU-SCICFI tulemuslikuks väljatöötamiseks vajalike ressursside hindamine;

   b. kriisijuhtimis- ja erandolukorra simulatsioonide väljatöötamine, mis hõlmab küberrünnete stsenaariume, et töötada välja sidekanalid;

   c. ühise sõnavara välja töötamine;

   d. ühtse küberintsidentide liigituse välja töötamine;

   e. turvalise ja usaldusväärsete teabejagamise kanalite loomine, sh varundus;

   f. kontaktpunktide kindlaks määramine;

   g. konfidentsiaalsuse küsimuste käsitlemine teabe jagamisel;

   h. finantssektori küberteadmust hõlmavad koostöö- ja teabejagamise algatused;

   i. tulemuslike aktiveerimis- ja eskaleerumisprotsesside välja töötamine olukorrateadlikkuse abil;

   j. raamistikus osalejate vastutusvaldkondade määratlemine;

   k. liideste loomine sektoriüleseks koostööks ning asjakohastel juhtudel koostööks kolmandate riikidega;

   l. sidusa teabe jagamise tagamine asjaomaste asutuste poolt üldsuse usalduse säilitamiseks;

   m. eelnevalt kindlaksmääratud sidekanalite loomine õigeaegseks infovahetuseks;

   n. asjakohaste simulatsioonide läbiviimine koordineerimisraamistikus, sh jurisdiktsioonideülesed testid ning koostöö kolmandate riikidega, ning hindamiste läbiviimine tähelepanekute tegemiseks ja raamistiku edasiarendamiseks;

   o. tõhusa infovahetuse tagamine ja vastumeetmed eksitava teabe levitamisele.

Soovitus B – EU-SCICFi konktaktpunktide määramine

Soovituse B osas kehtivad järgmised vastavuskriteeriumid.

1. Euroopa järelevalveasutused, EKP ja iga liikmesriik peab oma asjaomase riigi ametiasutusega kokku leppima ühtses lähenemises EU-SCICFi määratud kontaktpunktide nimekirja jagamise ja ajakohastamise osas.

2. Kontaktpunkti määramist tuleb hinnata, võttes arvesse direktiivi (EL) 2016/1148 kohaselt määratud ühtseid kontaktpunkte, mille liikmesriigid on nimetanud võrgu- ja infosüsteemide turvalisuse huvides selleks, et tagada piiriülene koostöö teiste liikmesriikide ning võrgu- ja infoturbe koostöörühmaga.

Soovitus C – liidu õigusraamistiku muutmine

Soovituse C osas määratletakse järgmised vastavuskriteeriumid.

Komisjon peab kaaluma, kas soovituse A kohaselt läbiviidud analüüsi tulemusel on vaja võtta meetmeid, sh muuta asjakohaseid liidu õigusakte, tagamaks, et Euroopa järelevalveasutused oma ühiskomitee kaudu ning koostöös EKP, ESRNi ja asjaomaste riigi ametiasutustega saavad EU-SCICFI arendada vastavalt soovituse A punktile 1 ning et Euroopa järelevalveasutused, EKP, ESRN ja asjaomased riigi ametiasutused ning teised asutused saavad osaleda koordineerimistegevustes ning tulemusliku EU-SCICFi tagamiseks piisavalt detailse ja järjepideva teabe vahetamisel.