EIROPAS
KOMISIJA

Briselē, 24.9.2020.
COM(2020) 595 final

2020/0266 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA

par finanšu sektora digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014 un (ES) Nr. 909/2014

(Dokuments attiecas uz EEZ)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

PASKAIDROJUMA RAKSTS

1. PRIEKŠLIKUMA KONTEKSTS

- Priekšlikuma pamatojums un mērķi

Šis priekšlikums ir daļa no digitālo finanšu dokumentu paketes — pasākumu kopuma, kas vēl vairāk nodrošinās un atbalstīs digitālo finanšu inovācijas un konkurētspējas potenciālu, vienlaikus mazinot no tā izrietošos riskus. Tas atbilst Komisijas prioritātēm — pielāgot Eiropu digitālajam laikmetam un veidot nākotnei gatavu ekonomiku, kas darbojas cilvēku labā. Digitālo finanšu dokumentu pakete ietver jaunu ES finanšu nozares digitālā finansējuma stratēģiju[1], kuras mērķis ir nodrošināt, ka ES izmanto digitālo revolūciju un virza to inovatīvu Eiropas tirgus dalībnieku vadībā, darot pieejamus digitālo finanšu ieguvumus patērētājiem un uzņēmumiem. Līdztekus šim priekšlikumam paketē ir iekļauts arī priekšlikums regulai par kriptoaktīvu tirgiem[2], priekšlikums regulai par sadalītās virsgrāmatas tehnoloģijas (SVT) tirgus infrastruktūras izmēģinājuma režīmu[3] un priekšlikums direktīvai, ar ko precizē vai groza atsevišķus savstarpēji saistītus ES finanšu pakalpojumu noteikumus[4]. Finanšu nozares digitalizācija un darbības noturība ir vienas monētas divas puses. Digitālās jeb informācijas un komunikācijas tehnoloģijas (IKT) rada kā iespējas, tā riskus. Tie ir labi jāizprot un jāpārvalda, īpaši spriedzes apstākļos.

Tādēļ politikas veidotāji un uzraugi arvien biežāk ir veltījuši uzmanību riskiem, kas izriet no paļaušanās uz IKT. Tie jo īpaši ir centušies stiprināt uzņēmumu noturību, nosakot standartus un koordinējot regulatīvo vai uzraudzības darbu. Šis darbs ir veikts gan starptautiskā, gan Eiropas līmenī, kā arī gan starpnozaru, gan vairāku atsevišķu nozaru līmenī, tai skaitā finanšu pakalpojumu nozarē.

Tomēr IKT riski vēl arvien rada riskus ES finanšu sistēmas darbības noturībai, veiktspējai un stabilitātei. Pēc 2008. gada finanšu krīzes veiktā reforma galvenokārt stiprināja ES finanšu nozares finansiālo noturību[5], pievēršoties IKT riskiem tikai netieši dažās jomās kā daļai no plašākas darbības risku novēršanas pasākumiem.

Lai gan ar ES finanšu pakalpojumu tiesību aktu izmaiņām, kas tika veiktas pēc krīzes, tika ieviests vienots noteikumu kopums, ko piemēroja lielai daļai ar finanšu pakalpojumiem saistīto risku, ar to netika pilnībā risināta digitālās darbības noturība. Šajā sakarā veiktajiem pasākumiem piemita vairākas īpašības, kas ierobežoja to efektivitāti. Piemēram, tie bieži bija izstrādāti kā minimālas saskaņošanas direktīvas vai uz principiem balstītas regulas, kas atstāja ievērojamas iespējas vienotajā tirgū piemērot atšķirīgas pieejas. Turklāt saistībā ar operacionālā riska segumu IKT riskiem ir tikusi veltīta tikai ierobežota vai nepilnīga uzmanība. Visbeidzot, šie pasākumi nozaru finanšu pakalpojumu tiesību aktos atšķiras. Tādēļ

---

1 Komisijas 2020. gada 23. septembra paziņojums Eiropas Parlamentam, Eiropadomei, Padomei, Eiropas Centrālajai bankai, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai par ES digitālā finansējuma stratēģiju, COM(2020) 591 final.

2 Priekšlikums Eiropas Parlamenta un Padomes regulai par kriptoaktīvu tirgiem un ar ko groza Direktīvu (ES) 2019/1937, COM(2020) 593 final.

3 Priekšlikums Eiropas Parlamenta un Padomes regulai par izmēģinājuma režīmu attiecībā uz tirgus infrastruktūrām, kuru pamatā ir sadalītās virsgrāmatas tehnoloģija, COM(2020) 594 final.

4 Priekšlikums Eiropas Parlamenta un Padomes direktīvai, ar ko groza Direktīvas 2006/43/EK, 2009/65/EK, 2009/138/EK, 2011/61/ES, 2013/36/ES, 2014/65/ES, (ES) 2015/2366 un (ES) 2016/2341, COM(2020) 596 final.

5 Dažādo pieņemto pasākumu pamatmērķis bija palielināt finanšu vienību kapitāla resursus un likviditāti, kā arī mazināt tirgus riskus un kredītriskus.

iejaukšanās Savienības līmenī pilnā mērā nesasniedza to, kas Eiropas finanšu vienībām bija vajadzīgs, lai pārvaldītu darbības riskus tā, lai izturētu IKT incidentus, reaģētu uz tiem un novērstu to radītās sekas. Tā arī nenodrošināja finanšu uzraudzības iestādēm vispiemērotākos rīkus, ar kuriem izpildīt to pilnvaras novērst no šo IKT risku īstenošanās izrietošo finanšu nestabilitāti.

Detalizētu un visaptverošu digitālās darbības noturības noteikumu neesība ES līmenī ir radījusi valstu regulatīvo iniciatīvu (piem., attiecībā uz digitālās darbības noturības testēšanu) un uzraudzības pieeju (piem., risinot atkarību no trešām personām, kas sniedz IKT pakalpojumus) izplatīšanos. Ņemot vērā IKT risku pārrobežu būtību, rīcībai dalībvalstu līmenī tomēr ir tikai ierobežota ietekme. Turklāt nekoordinētās valstu iniciatīvas ir radījušas pārklāšanos, nesakritības, prasību dublēšanos, augstas administratīvās un atbilstības nodrošināšanas izmaksas, jo sevišķi pārrobežu finanšu vienībām, vai arī to dēļ IKT riski nav atklāti un tādējādi arī nav novērsti. Šī situācija sadrumstalo vienoto tirgu, nelabvēlīgi ietekmē ES finanšu nozares stabilitāti un integritāti, kā arī apdraud patērētāju un ieguldītāju aizsardzību.

Tādēļ ir nepieciešams ieviest detalizētu un visaptverošu ES finanšu vienību digitālās darbības noturības sistēmu. Šī sistēma padziļinās vienotā noteikumu kopuma digitālo risku pārvaldības dimensiju. Tā jo īpaši uzlabos un racionalizēs to, kā finanšu vienības veic IKT riska pārvaldību, iedibinās IKT sistēmu padziļinātu testēšanu, palielinās uzraugu informētību par kiberriskiem un ar IKT saistītiem incidentiem, ar ko saskaras finanšu vienības, kā arī ieviesīs finanšu uzraudzības iestāžu pilnvaras pārraudzīt riskus, ko rada finanšu vienību atkarība no trešām personām, kas sniedz IKT pakalpojumus. Ar priekšlikumu tiks izveidots konsekvents mehānisms ziņošanai par incidentiem, kas palīdzēs mazināt administratīvo slogu finanšu vienībām, kā arī stiprināta uzraudzības efektivitāte.

- Saskanība ar pašreizējiem noteikumiem konkrētajā politikas jomā

Šis priekšlikums ir daļa no plašāka darba, kas tiek veikts Eiropas un starptautiskajā līmenī, lai stiprinātu finanšu pakalpojumu kiberdrošību un novērstu plašākus darbības riskus[6].

Tas ir arī kā atbilde uz Eiropas uzraudzības iestāžu (EUI) 2019. gada kopīgajiem tehniskajiem ieteikumiem[7], kuros izteikts aicinājums īstenot saskaņotu pieeju IKT riskam finanšu nozarē un ieteikts Komisijai proporcionāli stiprināt finanšu pakalpojumu nozares digitālās darbības noturību ar Savienības specifisku nozares iniciatīvu. EUI ieteikums bija atbilde uz Komisijas 2018. gada Finanšu tehnoloģijas rīcības plānu[8].

- Saskanība ar citām Savienības politikas jomām

Kā savās politikas pamatnostādnēs[9] un paziņojumā par Eiropas digitālās nākotnes veidošanu[10] ir norādījusi Komisijas priekšsēdētāja Urzula fon der Leiena, Eiropai ir svarīgi izmantot visas digitālā laikmeta priekšrocības un stiprināt tās rūpniecību un inovācijas spējas drošuma un

---

6 Bāzeles Banku uzraudzības komiteja. *Cyber-resilience: Range of practices*, 2018. gada decembris, un *Principles for sound management of operational risk (PSMOR)*, 2014. gada oktobris.

7 Eiropas uzraudzības iestāžu kopīgais ieteikums Eiropas Komisijai par nepieciešamību uzlabot tiesību aktus saistībā ar IKT riska pārvaldības prasībām ES finanšu nozarē, JC 2019 26 (2019).

8 Eiropas Komisija. "Finanšu tehnoloģijas rīcības plāns", COM(2018) 109 final.

9 Priekšsēdētāja Urzula fon der Leiena. "Politikas pamatnostādnes nākamajai Eiropas Komisijai (2019–2024)", https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_lv.pdf.

10 Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai "Eiropas digitālās nākotnes veidošana", COM(2020) 67 final.

ētiskuma robežās. Eiropas Datu stratēģijā[11] ir paredzēti četri pīlāri — datu aizsardzība, pamattiesības, drošums un kiberdrošība — kā būtiski priekšnoteikumi sabiedrībai, kam datu izmantošana sniedz iespējas. Pēdējā laikā Eiropas Parlaments strādā pie ziņojuma par digitālajām finansēm, kurā cita starpā izteikts aicinājums izveidot vienotu pieeju finanšu sektora kibernoturībai[12]. Tiesiskais regulējums, kas stiprina ES finanšu vienību digitālās darbības noturību, atbilst šiem politikas mērķiem. Priekšlikumā atbalstīta arī rīcībpolitika, kas ir vērsta uz atgūšanos no koronavīrusa, jo tas nodrošinātu, ka lielāka paļaušanās uz digitālajām finansēm iet roku rokā ar darbības noturību.

Iniciatīva saglabātu ieguvumus, kas saistīti ar kiberdrošības horizontālo sistēmu (piemēram, Tīklu un informācijas sistēmu drošības direktīva jeb TID direktīva), paturot finanšu nozari tās darbības jomā. Finanšu nozare būtu cieši saistīta ar TID sadarbības struktūru, un finanšu uzraudzības iestādes spētu apmainīties ar attiecīgu informāciju esošajā TID ekosistēmā. Iniciatīva atbilstu Eiropas kritiskās infrastruktūras (EKI) direktīvai, kas pašlaik tiek pārskatīta, lai uzlabotu kritisko infrastruktūru aizsardzību un noturību pret apdraudējumiem, kas nav saistīti ar kiberuzbrukumiem. Visbeidzot, šis priekšlikums pilnībā atbilst Drošības savienības stratēģijai[13], kurā izteikts aicinājums izstrādāt iniciatīvu par digitālās darbības noturību finanšu nozarē, ņemot vērā tās augsto atkarību no IKT pakalpojumiem un augsto neaizsargātību pret kiberuzbrukumiem.

2. JURIDISKAIS PAMATS, SUBSIDIARITĀTE UN PROPORCIONALITĀTE

- Juridiskais pamats

Šis regulas priekšlikums ir balstīts uz LESD 114. pantu.

Ar to tiek novērsti šķēršļi, kā arī uzlabota finanšu pakalpojumu iekšējā tirgus izveide un darbība, saskaņojot noteikumus, kas piemērojami IKT riska pārvaldībai, ziņošanai, testēšanai un ar trešo personu saistītajam IKT riskam. Pašreizējās likumdošanas un uzraudzības, kā arī valsts un ES līmeņu atšķirības šajā jomā ir šķēršļi finanšu pakalpojumu vienotajam tirgum, jo finanšu vienības, kas veic pārrobežu darbības, saskaras ar atšķirīgām regulatīvām prasībām vai gaidām uzraudzības jomā, kas nepārklājas un var kavēt tām izmantot brīvību veikt uzņēmējdarbību un sniegt pakalpojumus. Atšķirīgi noteikumi arī kropļo konkurenci starp viena veida finanšu vienībām dažādās dalībvalstīs. Turklāt jomās, kurās saskaņošana nav notikusi vai ir daļēja vai ierobežota, tādu atšķirīgu valsts noteikumu vai pieeju izstrādei, kas vai nu jau ir spēkā, vai atrodas pieņemšanas un īstenošanas procesā valsts līmenī, var būt atturoša ietekme uz finanšu pakalpojumu vienotā tirgus brīvībām. Tas tā jo īpaši ir attiecībā uz digitālās darbības testēšanas satvariem un kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, pārraudzību.

Tā kā priekšlikums ietekmē vairākas Eiropas Parlamenta un Padomes direktīvas, kas ir pieņemtas saskaņā ar LESD 53. panta 1. punktu, vienlaikus tiek pieņemts priekšlikums direktīvai, lai atspoguļotu šajās direktīvās izdarāmos grozījumus.

---

[11] Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai "Eiropas Datu stratēģija", COM(2020) 66 final.

[12] Ziņojums ar ieteikumiem Komisijai par digitālajām finansēm: jauni ar kriptoaktīviem saistīti riski — regulējuma un uzraudzības problēmas finanšu pakalpojumu, iestāžu un tirgu nozarē (2020/2034(INL)), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en.

[13] Komisijas paziņojums Eiropas Parlamentam, Eiropadomei, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai "ES Drošības savienības stratēģija", COM(2020) 605 final.

- Subsidiaritāte

Augstā finanšu pakalpojumu savstarpējās savienojamības pakāpe, nozīmīga finanšu vienību pārrobežu darbība un plaša finanšu nozares kopējā atkarība no trešām personām, kas sniedz IKT pakalpojumus, prasa nodrošināt spēcīgu digitālās darbības noturību, kas ES finanšu tirgu stabilitātes saglabāšanai ir kopīgu interešu jautājums. Atšķirības, kas rodas no nevienmērīgiem vai daļējiem režīmiem, pārklāšanās vai vairākām prasībām, ko piemēro vienām un tām pašām finanšu vienībām, kuras darbojas pāri robežām vai kurām ir vairākas atļaujas[14] visā vienotajā tirgū, var efektīvi risināt tikai Savienības līmenī.

Ar šo priekšlikumu tiek saskaņots digitālās darbības komponents dziļi integrētā un savstarpēji savienotā nozarē, kas jau šobrīd vairumā citu būtisko jomu izmanto vienotu noteikumu kopumu un uzraudzību. Tādos jautājumos kā ziņošana par incidentiem, kas saistīti ar IKT, vienīgi Savienības līmenī saskaņoti noteikumi varētu mazināt administratīvo slogu un finanšu izmaksas, ko rada ziņošana dažādām Savienības un valstu iestādēm par vienu un to pašu ar IKT saistīto incidentu. ES rīcība ir nepieciešama arī, lai sekmētu pārrobežu iestāžu padziļinātas digitālās darbības noturības testēšanas rezultātu savstarpēju atzīšanu, kas, nepastāvot Savienības noteikumiem, dažādās dalībvalstīs tiek vai varētu tikt pakļauta atšķirīgam regulējumam. Tikai rīcība Savienības līmenī var novērst dalībvalstu ieviestās atšķirības testēšanas pieejā. ES līmeņa rīcība ir nepieciešama arī, lai risinātu to, ka trūkst pienācīgu pārraudzības pilnvaru, lai uzraudzītu ar trešām personām, kas sniedz IKT pakalpojumus, saistītos riskus, ieskaitot ES finanšu nozares koncentrācijas un kaitīgas ietekmes riskus.

- Proporcionalitāte

Ar ierosinātajiem noteikumiem paredz tikai to, kas nepieciešams, lai sasniegtu priekšlikuma mērķus. Tie aptver tikai aspektus, kurus dalībvalstis nevar sasniegt saviem spēkiem un kuru administratīvais slogs un izmaksas ir samērīgas ar sasniedzamajiem konkrētajiem un vispārīgajiem mērķiem.

Samērīgumu nosaka pēc darbības jomas un intensitātes, izmantojot kvalitatīvus un kvantitatīvus novērtēšanas kritērijus. To mērķis ir nodrošināt, ka, lai gan jaunie noteikumi aptver visas finanšu vienības, tie vienlaikus ir pieskaņoti riskiem un vajadzībām, kas izriet no vienību lieluma un darījumdarbības profila sevišķajām īpašībām. Proporcionalitāte ir ietverta arī noteikumos par IKT riska pārvaldību, digitālās darbības noturības testēšanu, ziņošanu par būtiskiem ar IKT saistītiem incidentiem un kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, pārraudzību.

- Juridiskā instrumenta izvēle

Pasākumiem, kas nepieciešami, lai regulētu IKT riska pārvaldību, ar IKT saistītu incidentu paziņošanu, testēšanu un kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, pārraudzību, ir jābūt ietvertiem regulā, lai nodrošinātu, ka detalizētās prasības ir efektīvi un tieši piemērojamas vienveidīgi, neskarot proporcionalitāti un šajā regulā paredzētos īpašos noteikumus. Konsekventa digitālo operacionālo risku novēršana palīdz uzlabot uzticēšanos finanšu sistēmai un uztur tās stabilitāti. Tā kā regulas izmantošana palīdz mazināt regulatīvo sarežģītību, sekmē uzraudzības konverģenci un palielina juridisko noteiktību, šī regula arī

[14] Vienai un tai pašai finanšu vienībai var būt banku darbības, ieguldījumu brokeru sabiedrības un maksājumu iestādes atļaujas, kuras izdevuši dažādas uzraudzības iestādes vienā vai vairākās dalībvalstīs.

sekmē finanšu vienību atbilstības nodrošināšanas izmaksu ierobežošanu, īpaši finanšu vienībām, kas darbojas pārrobežu vidē, tādējādi palīdzot novērst konkurences izkropļojumus.

Ar regulu tiek arī novērstas tiesību aktu nesakritības un nevienāda valstu regulatīvā vai uzraudzības pieeja attiecībā uz IKT risku, tādējādi novēršot šķēršļus izveidot finanšu pakalpojumu vienoto tirgu, jo īpaši šķēršļus pārrobežu finanšu vienību brīvībai veikt uzņēmējdarbību un sniegt pakalpojumus.

Visbeidzot, vienotais noteikumu kopums galvenokārt ir izstrādāts, izmantojot regulas, un tā aktualizēšanai ar digitālās darbības noturības komponentu jāizvēlas tāds pats juridiskais instruments.

3. *EX POST* IZVĒRTĒJUMU, APSPRIEŠANOS AR IEINTERESĒTAJĀM PERSONĀM UN IETEKMES NOVĒRTĒJUMU REZULTĀTI

- *Ex post* izvērtējumi / spēkā esošo tiesību aktu atbilstības pārbaudes

Neviens Savienības finanšu pakalpojumu tiesību akts līdz šim nav bijis orientēts uz darbības noturību un nav visaptveroši risinājis digitalizācijas radītos riskus — pat tie tiesību akti, kuru noteikumi vispārīgāk regulē operacionālā riska dimensiju ar IKT risku kā apakškomponentu. Līdz šim Savienības iejaukšanās ir palīdzējusi risināt pēc 2008. gada finanšu krīzes pastāvošās vajadzības un problēmas: kredītiestādēm nebija pietiekama kapitāla, finanšu tirgi nebija pietiekami integrēti, un līdzšinējā saskaņošana bija bijusi minimāla. Tolaik IKT risks netika uzskatīts par prioritāru, tādēļ dažādu finanšu apakšnozaru tiesiskais regulējums ir attīstījies nesaskaņoti. Tomēr ar Savienības rīcību ir sasniegts mērķis — nodrošināt finanšu stabilitāti un izveidot saskaņotu prudenciālo un tirgus rīcības noteikumu vienotu kopumu, kas tiek piemērots visas ES finanšu vienībām. Tā kā faktori, kas iepriekš noteica Savienības likumdevēja iejaukšanos, nenodrošināja īpašus vai visaptverošus noteikumus, kas paredzēti, lai īpaši pievērstos digitālo tehnoloģiju izplatītajai lietošanai un no tās izrietošajiem riskiem finanšu nozarei, tieša izvērtējuma veikšana, šķiet, ir apgrūtināta. Katrā šīs regulas pīlārā ir atspoguļots netiešs izvērtējums un no tā izrietošie tiesību aktu grozījumi.

- Apspriešanās ar ieinteresētajām personām

Komisija visā šā priekšlikuma izstrādes gaitā ir apspriedusies ar ieinteresētajām personām, konkrēti:

i) Komisija īstenoja īpašu publisku sabiedrisko apspriešanu (no 2019. gada 19. decembra līdz 2020. gada 19. martam)[15];

ii) Komisija apspriedās ar sabiedrību, veicot sākotnējo ietekmes novērtējumu (no 2019. gada 19. decembra līdz 2020. gada 16. janvārim)[16];

iii) Komisijas dienesti divos gadījumos konsultējās ar dalībvalstu ekspertiem ekspertu grupā banku, maksājumu un apdrošināšanas jomā (*EGBPI*) (2020. gada 18. maijs un 2020. gada 16. jūlijs)[17];

[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation.

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-.

iv) Komisijas dienesti digitālās darbības noturībai veltīja īpašu tīmekļsemināru (2020. gada 19. maijs), kas ir daļa no digitālajām finansēm veltītajiem informatīvajiem pasākumiem "*Digital Finance Outreach* 2020".

Sabiedriskās apspriešanas mērķis bija informēt Komisiju par potenciālā ES starpnozaru digitālās darbības noturības regulējuma izveidi finanšu pakalpojumu jomā. Atbildes liecināja par plašu atbalstu tam, lai tiktu ieviesta īpaša sistēma ar pasākumiem, kas vērsti uz četrām apspriešanā iekļautajām jomām, vienlaikus uzsverot vajadzību nodrošināt proporcionalitāti un rūpīgi skatīt un izskaidrot mijiedarbību ar TID direktīvas horizontālajiem noteikumiem. Komisija uz sākotnējo ietekmes novērtējumu saņēma divas atbildes, kurās respondenti pievērsās konkrētiem aspektiem, kas saistīti ar viņu darbības jomu.

Dalībvalstis 2020. gada 18. maijā organizētajā *EGPBI* sanāksmē pauda lielu atbalstu finanšu nozares digitālās darbības noturības stiprināšanai, izmantojot pasākumus, kas paredzēti atbilstīgi četriem Komisijas norādītajiem elementiem. Dalībvalstis arī uzsvēra nepieciešamību skaidri formulēt jaunos noteikumus kopā ar noteikumiem par operacionālo risku (ES tiesību aktos par finanšu pakalpojumiem) un horizontālajiem noteikumiem par kiberdrošību (TID direktīva). Otrās sanāksmes laikā dažas dalībvalstis uzsvēra nepieciešamību nodrošināt proporcionalitāti un ņemt vērā mazo uzņēmumu vai lielāku grupu meitasuzņēmumu īpašo situāciju, kā arī vajadzību pēc stingrām pilnvarām pārraudzībā iesaistītajām VKI.

Priekšlikuma pamatā ir arī atgriezeniskā saite, kas iegūta sanāksmēs ar ieinteresētajām personām un ES iestādēm un institūcijām. Ieinteresētās personas, tostarp trešās personas, kas sniedz IKT pakalpojumus, kopumā to ir atbalstījušas. Saņemtās atgriezeniskās saites analīze liecina par aicinājumu saglabāt proporcionalitāti, noteikumu izstrādē ievērojot uz principiem un risku balstītu pieeju. No iestāžu puses vislielāko ieguldījumu sniedza Eiropas Sistēmisko risku kolēģija (ESRK), EUI, Eiropas Savienības Kiberdrošības aģentūra (*ENISA*) un Eiropas Centrālā banka (ECB), kā arī dalībvalstu kompetentās iestādes.

- Ekspertu atzinumu pieprasīšana un izmantošana

Sagatavojot šo priekšlikumu, Komisija izmantoja no atzītiem avotiem iegūtus kvalitatīvus un kvantitatīvus pierādījumus, tostarp abus EUI kopīgos tehniskos ieteikumus. Tos papildināja konfidenciāli un publiski pieejami ziņojumi no uzraudzības iestādēm, starptautiskām standartizācijas iestādēm un vadošajiem pētniecības institūtiem, kā arī kvantitatīvs un kvalitatīvs ieguldījumu no identificētām visas pasaules finanšu nozares ieinteresētajām personām.

- Ietekmes novērtējums

Šim priekšlikumam ir pievienots ietekmes novērtējums[18], kas 2020. gada 29. aprīlī tika iesniegts Regulējuma kontroles padomei (RKP), bet 2020. gada 29. maijā tika apstiprināts. RKP ieteica veikt uzlabojumus dažās jomās ar mērķi: i) sniegt vairāk informācijas par to, kā tiktu nodrošināta proporcionalitāte; ii) labāk uzsvērt, cik lielā mērā vēlamais risinājums atšķiras no EUI kopīgajiem tehniskajiem ieteikumiem un kādēļ šis risinājums ir optimālākais;

---

17 https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en.

18 Komisijas dienestu darba dokuments — Ietekmes novērtējuma ziņojums, kas pievienots dokumentam "Eiropas Parlamenta un Padomes Regula par digitālās darbības noturību finanšu nozarē un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014 un (ES) Nr. 909/2014, SWD(2020) 198, 24.9.2020.

un iii) papildus uzsvērt, kā priekšlikums mijiedarbojas ar spēkā esošajiem ES tiesību aktiem, tostarp ar noteikumiem, kas pašlaik tiek pārskatīti. Ietekmes novērtējums tika pielāgots, lai risinātu šos jautājumus, ņemot vērā arī RKP sīkākas piezīmes.

Komisija apsvēra vairākus politikas risinājumus digitālās darbības noturības regulējuma izveidei:

- "nedarīt neko" — darbības noturības noteikumi arī turpmāk tiktu noteikti ar pašreizējo nesaskanīgo ES finanšu pakalpojumu noteikumu kopumu, daļēji ar TID direktīvu, kā arī esošajiem vai nākotnes valstu noteikumiem;
- 1. risinājums — stiprināt kapitāla rezerves: lai palielinātu finanšu vienību spēju absorbēt zaudējumus, kas varētu rasties digitālās darbības noturības neesības dēļ, tiktu ieviestas papildu kapitāla rezerves;
- 2. risinājums — ieviest finanšu pakalpojumu digitālās darbības noturības aktu: nodrošināt visaptverošu regulējumu ES līmenī ar konsekventiem noteikumiem, lai risinātu visu regulēto finanšu vienību digitālās darbības noturības vajadzības un izveidotu to trešo personu pārraudzības sistēmu, kas sniedz kritiski svarīgus IKT pakalpojumus;
- 3. risinājums — finanšu pakalpojumu digitālās darbības noturības akts apvienojumā ar to trešo personu centralizētu uzraudzību, kas sniedz kritiski svarīgus IKT pakalpojumus: papildus digitālās darbības noturības aktam (2. risinājums) tiktu izveidota jauna iestāde, lai uzraudzītu, kā trešās personas sniedz IKT pakalpojumus.

Tika izraudzīts otrais risinājums, jo ar to efektīvi, lietderīgi un saskanīgi ar citiem Savienības politikas pasākumiem tiek sasniegta lielākā daļa iecerēto mērķu. Šo risinājumu izvēlējušās arī lielākā daļa ieinteresēto personu.

Izvēlētais risinājums radītu kā vienreizējas, tā regulāras izmaksas[19]. Vienreizējās izmaksas galvenokārt veido ieguldījumi IT sistēmās, tādēļ tās ir grūti izteikt kvantitatīvi, jo uzņēmumu sarežģītās IT vides un jo īpaši to mantotās IT sistēmas pēc to stāvokļa atšķiras. Tomēr jebkurā gadījumā lieliem uzņēmumiem šīs izmaksas, visticamāk, būs ierobežotas, jo tie jau ir veikuši nozīmīgus ieguldījumus IKT. Paredzams, ka arī mazākiem uzņēmumiem radīsies ierobežotas izmaksas, jo tiem tiks piemēroti samērīgi pasākumi, ņemot vērā to zemāko risku.

Izvēlētā risinājuma ekonomiskā, sociālā un vidiskā ietekme uz finanšu pakalpojumu nozarē strādājošiem MVU būtu pozitīva. Ar priekšlikumu tiks panākts, ka MVU ir skaidri zināms, kuri noteikumi uz tiem attiecas, tādējādi samazinot atbilstības nodrošināšanas izmaksas.

Izvēlētais politikas risinājums galveno sociālo ietekmi atstātu uz patērētājiem un ieguldītājiem. Augstāks ES finanšu sistēmas digitālās darbības noturības līmenis samazinātu incidentu skaitu un vidējās izmaksas. Sabiedrība kopumā iegūtu no lielākas uzticēšanās finanšu pakalpojumu nozarei.

Visbeidzot, runājot par vidisko ietekmi, izvēlētais politikas risinājums mudinātu labāk izmantot jaunākās paaudzes IKT infrastruktūru un pakalpojumus, kas, domājams, kļūs ilgtspējīgāki no vides viedokļa.

- Normatīvā atbilstība un vienkāršošana

[19] Turpat, 89.–94. lpp.

Ja tiktu atceltas prasības paziņot ar IKT saistītus incidentus, kas savstarpēji pārklājas, tiktu samazināts administratīvais slogs un ar to saistītās izmaksas. Turklāt saskaņotas digitālās darbības noturības pārbaudes ar savstarpēju atzīšanu visā vienotajā tirgū samazinās izmaksas, jo īpaši pārrobežu uzņēmumiem, kuri citādi varētu saskarties ar vairākkārtējiem testiem visās dalībvalstīs.[20]

- Pamattiesības

ES ir apņēmusies nodrošināt augstus standartus pamattiesību aizsardzības jomā. Visas brīvprātīgas informācijas apmaiņas vienošanās starp finanšu vienībām, ko veicina šī regula, tiktu veiktas uzticamā vidē, pilnībā ievērojot Savienības datu aizsardzības noteikumus, jo īpaši Eiropas Parlamenta un Padomes Regulu (ES) 2016/679[21], sevišķi gadījumos, kad personas datu apstrāde ir nepieciešama personas datu pārziņa leģitīmo interešu ievērošanai.

4. IETEKME UZ BUDŽETU

Runājot par ietekmi uz budžetu, jāatzīst, ka, tā kā pašreizējā regula paredz plašāku EUI lomu, izmantojot pilnvaras, kas tām piešķirtas, lai pienācīgi pārraudzītu kritiski svarīgas trešās personas, kas IKT pakalpojumus, priekšlikums ietvertu plašāku resursu izmantošanu, jo īpaši, lai izpildītu pārraudzības uzdevumus (piemēram, pārbaudes uz vietas un tiešsaistē, revīzijas) un izmantotu personālu, kam ir īpašas zināšanas par IKT drošību.

Šo izmaksu apjoms un sadalījums būs atkarīgs no EUI jauno pārraudzības pilnvaru apjoma un (precīziem) veicamajiem uzdevumiem. Attiecībā uz jaunu personāla resursu nodrošināšanu EBI, EVTI un EAAPI kopā būs nepieciešami 18 pilnas slodzes darbinieki (PSE) — 6 PSE katrai iestādei — kad sāksies dažādu priekšlikuma noteikumu piemērošana (paredzamais apmērs — 15,71 miljoni EUR par laikposmu no 2022. līdz 2027. gadam). EUI radīsies arī papildu IT izmaksas, komandējuma izdevumi par pārbaudēm uz vietas un tulkošanas izmaksas (aprēķinātas 12 miljonu EUR apmērā par laikposmu no 2022. līdz 2027. gadam), kā arī citi administratīvie izdevumi (aprēķināti 2,48 miljonu EUR apmērā par laika periodu no 2022. līdz 2027. gadam). Tādēļ paredzamā kopējā ietekme uz izmaksām 2022.–2027. gadā ir aptuveni 30,19 miljoni EUR.

Jānorāda arī tas, ka, lai gan tiešai pārraudzībai nepieciešamais darbinieku skaits (piemēram, jauni darbinieki un citi izdevumi, kas saistīti ar jaunajiem uzdevumiem) laika gaitā būs atkarīgs no tā, kā mainīsies pārraugāmo kritiski svarīgo trešo personu, kas sniedz IKT pakalpojumus, skaits un lielums, attiecīgos izdevumus pilnībā finansēs no maksām, kas iekasētas no šiem tirgus dalībniekiem. Tāpēc nav paredzēta ietekme uz ES budžeta apropriācijām (izņemot attiecībā uz papildu personālu), jo šīs izmaksas pilnībā finansēs no maksām.

Priekšlikuma finansiālā ietekme un ietekme uz budžetu sīkāk izskaidrota šim priekšlikumam pievienotajā tiesību akta finanšu pārskatā.

5. CITI ELEMENTI

- Īstenošanas plāni un uzraudzīšanas, izvērtēšanas un ziņošanas kārtība

---

[20] Turpat.

[21] Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

Priekšlikums ietver vispārēju plānu, kā uzraudzīt un izvērtēt ietekmi uz konkrētajiem mērķiem, un tas paredz, ka Komisijai vismaz trīs gadus pēc tā stāšanās spēkā ir jāveic pārskatīšana un jāziņo Eiropas Parlamentam un Padomei par galvenajiem konstatējumiem.

Pārskatīšana ir veicama atbilstoši Komisijas labāka regulējuma pamatnostādnēm.

- Detalizēts konkrētu priekšlikuma noteikumu skaidrojums

Priekšlikums ir strukturēts ap vairākām galvenajām politikas jomām — svarīgiem savstarpēji saistītiem pīlāriem, kuri pēc vienošanās tiek iekļauti Eiropas un starptautiskajos norādījumos un labākajā praksē un kuru mērķis ir uzlabot finanšu nozares kibernoturību un darbības noturību.

Regulas darbības joma un obligāto pasākumu proporcionalitātes piemērošana (2. pants)

Lai nodrošinātu vienveidīgumu attiecībā uz finanšu nozarē piemērojamajām IKT riska pārvaldības prasībām, regula aptver virkni Savienības līmenī regulētu finanšu vienību, proti, kredītiestādes, maksājumu iestādes, elektroniskās naudas iestādes, ieguldījumu brokeru sabiedrības, kriptoaktīvu pakalpojumu sniedzējus, centrālos vērtspapīru depozitārijus, centrālos darījumu partnerus (*CCP*), tirdzniecības vietas, darījumu reģistrus, alternatīvo ieguldījumu fondu pārvaldniekus un pārvaldības sabiedrības, datu paziņošanas pakalpojumu sniedzējus, apdrošināšanas un pārapdrošināšanas sabiedrības, apdrošināšanas starpniekus, pārapdrošināšanas starpniekus, apdrošināšanas papildpakalpojuma starpniekus, arodpensiju iestādes, kredītreitingu aģentūras, obligātos revidentus, revīzijas uzņēmumus, kritiski svarīgu etalonu administratorus un kolektīvās finansēšanas pakalpojumu sniedzējus.

Šāda darbības joma sekmē visu IKT jomas riska pārvaldības komponentu viendabīgu un saskaņotu piemērošanu, vienlaikus aizsargājot vienlīdzīgus konkurences apstākļus finanšu vienību starpā no IKT riska regulatīvo pienākumu viedokļa. Vienlaikus regulā ir atzīts, ka starp finanšu vienībām pastāv nozīmīgas atšķirības attiecībā uz to lielumu, darījumdarbības profilu vai pakļautību digitālajam riskam. Tā kā lielākām finanšu vienībām ir vairāk resursu, tikai finanšu vienībām, kas neatbilst mikrouzņēmuma statusam, ir pienākums, piemēram, izveidot sarežģītu pārvaldības kārtību, īpašas vadības funkcijas, veikt padziļinātu novērtējumu pēc būtiskām tīklu un informācijas sistēmas infrastruktūras izmaiņām, regulāri veikt mantotu IKT sistēmu riska analīzi, paplašināt darbības nepārtrauktības, reaģēšanas un seku novēršanas plānu testēšanu, lai aptvertu scenārijus, kuros notiek pārslēgšanās starp primāro IKT infrastruktūru un rezerves mehānismiem. Turklāt tikai finanšu vienībām, kas atzītas par nozīmīgām padziļinātas digitālās darbības noturības testēšanas mērķiem, būs pienākums veikt draudu vadītus ielaušanās testus.

Neraugoties uz šo plašo tvērumu, tas nav izsmeļošs. Šajā regulā nav ietverti sistēmas operatori, kā definēts Direktīvas 98/26/EK[22] par norēķinu galīgumu maksājumu un vērtspapīru norēķinu sistēmās (NGD) 2. panta p) punktā, kā arī neviens sistēmas dalībnieks, ja vien šis dalībnieks pats nav Savienības līmenī regulēta finanšu vienība un uz to šī regula neattiecas pati par sevi (proti, kredītiestāde, ieguldījumu brokeru sabiedrība, *CCP*). Turklāt

[22] Eiropas Parlamenta un Padomes Direktīva 98/26/EK (1998. gada 19. maijs) par norēķinu galīgumu maksājumu un vērtspapīru norēķinu sistēmās (OV L 166, 11.6.1998., 45. lpp.).

darbības jomā neietilpst arī Savienības emisiju kvotu reģistrs, kas saskaņā ar Direktīvu 2003/87/EK[23] darbojas Eiropas Komisijas aizgādībā.

Attiecībā uz šādiem NGD izņēmumiem ņemta vērā nepieciešamība turpmāk pārskatīt juridiskus un politiskus jautājumus, kas skar NGD sistēmas operatorus un dalībniekus, vienlaikus pienācīgi ņemot vērā to, kā spēkā esošās sistēmas ietekmē centrālo banku pārvaldītās maksājumu sistēmas[24]. Tā kā šie jautājumi var būt saistīti ar aspektiem, kas joprojām ir nošķirti no šīs regulas jautājumiem, Komisija turpinās izvērtēt nepieciešamību un ietekmi, ko radītu šīs regulas darbības jomas tālāka paplašināšana, attiecinot to uz vienībām un IKT infrastruktūrām, kas pašlaik nav tās kompetencē.

Ar pārvaldību saistītas prasības (4. pants)

Šīs regulas mērķis ir labāk saskaņot finanšu vienību darījumdarbības stratēģijas un IKT riska pārvaldības norisi. Šim nolūkam vadības struktūrai būs jāsaglabā nozīmīga un aktīva loma IKT riska pārvaldības sistēmas vadībā un jātiecas uz stingras kiberhigiēnas ievērošanu. Vadības struktūras pilnīga atbildība par finanšu vienības IKT riska pārvaldību būs visaptverošs princips, kas būs sīkāk jāizsaka kā specifisku prasību kopums, piemēram, attiecībā uz skaidru lomu un pienākumu piešķiršanu visām ar IKT saistītajām funkcijām, nepārtrauktu iesaistīšanos IKT riska pārvaldības uzraudzības kontrolē, kā arī pilnu apstiprināšanas un kontroles procesu spektru un atbilstošu IKT ieguldījumu un apmācību iedalīšanu.

IKT riska pārvaldības prasības (5.–14. pants)

Atbilstīgi EUI kopīgajiem tehniskajiem ieteikumiem digitālās darbības noturība balstās uz vairāku IKT riska pārvaldības sistēmai noteiktu galveno principu un prasību kopumu. Šīs prasības, kuru izstrādi ir sekmējuši attiecīgi starptautiski, valsts un nozares noteikti standarti, nostādnes un ieteikumi, attiecas uz konkrētām IKT riska pārvaldības funkcijām (identifikāciju, aizsardzību un profilaksi, atklāšanu, reaģēšanu un seku novēršanu, mācīšanos un attīstību, saziņu). Lai neatpaliktu no strauji mainīgās kiberdraudu vides, finanšu vienībām ir pienākums izveidot un uzturēt noturīgas IKT sistēmas un rīkus, kas mazina IKT riska ietekmi, pastāvīgi identificēt visus IKT riska avotus, izveidot aizsardzības un profilakses pasākumus, nekavējoties atklāt anomālas darbības, ieviest īpašu un visaptverošu darbības nepārtrauktības politiku un negadījuma seku novēršanas plānus kā darbības nepārtrauktības politikas neatņemamu daļu. Pēdējie no minētajiem komponentiem ir nepieciešami, lai operatīvi novērstu ar IKT saistīto incidentu, jo īpaši kiberuzbrukumu, sekas, ierobežojot kaitējumu un par prioritāru nosakot drošu darbības atsākšanu. Ar regulu kā tādu netiek noteikti konkrēti standarti — tā balstās uz Eiropas un starptautiski atzītiem tehniskajiem standartiem vai nozares labāko praksi, ciktāl tā pilnībā atbilst uzraudzības norādījumiem par šādu starptautisko standartu izmantošanu un iekļaušanu. Regula aptver arī fiziskās infrastruktūras integritāti, drošumu un noturību, kā arī tādu objektu integritāti, drošumu un noturību, kas atbalsta tehnoloģiju izmantošanu un attiecīgos ar IKT saistītos procesus un cilvēkus, un tā ir daļa no finanšu vienības darbības digitālā pēdas nospieduma.

Ar IKT saistīto incidentu paziņošana (15.–20. pants)

---

[23] Eiropas Parlamenta un Padomes Direktīva 2003/87/EK (2003. gada 13. oktobris), ar kuru nosaka sistēmu siltumnīcas efektu izraisošo gāzu emisijas kvotu tirdzniecībai Savienībā un groza Padomes Direktīvu 96/61/EK (OV L 275, 25.10.2003., 32. lpp.).

[24] Jo īpaši Eiropas Centrālās bankas Regula (ES) Nr. 795/2014 (2014. gada 3. jūlijs) par sistēmiski nozīmīgu maksājumu sistēmu pārraudzību.

Ar IKT saistīto incidentu paziņošanas saskaņošanu un racionalizāciju panāk, pirmkārt, ar vispārēju prasību finanšu vienībām izveidot un īstenot pārvaldības procesu ar IKT saistīto incidentu uzraudzībai un reģistrēšanai, kam seko pienākums tos klasificēt atbilstīgi regulā sīkāk izklāstītiem un EUI tālāk izstrādātajiem kritērijiem, pēc kuriem nosaka būtiskuma robežvērtības. Otrkārt, kompetentajām iestādēm ir jāziņo tikai par tiem ar IKT saistītajiem incidentiem, kas ir atzīti par būtiskiem. Ziņošana būtu jāveic, izmantojot vienotu veidni un ievērojot EUI izstrādātu saskaņotu procedūru. Finanšu vienībām būtu jāiesniedz sākotnējie, starpposma un gala ziņojumi, kā arī jāinformē lietotāji un klienti, kuru finanšu intereses ir vai varētu būt skāris incidents. Kompetentajām iestādēm būtu jāsniedz attiecīgas sīkākas ziņas par incidentiem citām institūcijām vai iestādēm: EUI, ECB un saskaņā ar Direktīvu (ES) 2016/1148 izraudzītajiem vienotajiem kontaktpunktiem.

Lai uzsāktu dialogu starp finanšu vienībām un kompetentajām iestādēm, kas palīdzētu mazināt ietekmi un noteikt piemērotus korektīvos pasākumus, ziņošana par būtiskiem ar IKT saistītiem incidentiem būtu jāpapildina ar uzrauga atgriezenisko saiti un norādījumiem.

Visbeidzot, EUI, ECB un *ENISA* kopīgā ziņojumā, kurā būtu vērtēta iespējamība izveidot vienotu ES centrmezglu, kuram finanšu vienības ziņotu par būtiskiem ar IKT saistītiem incidentiem, būtu sīkāk jāanalizē iespēja Savienības līmenī centralizēt ar IKT saistītu incidentu paziņošanu.

Digitālās darbības noturības testēšana (21.–24. pants)

IKT riska pārvaldības sistēmā ietvertās spējas un funkcijas ir periodiski jātestē attiecībā uz gatavību un spēju identificēt vājās vietas, trūkumus un nepilnības, kā arī nekavējoties īstenot korektīvos pasākumus. Šī regula ļauj proporcionāli piemērot digitālās darbības noturības testēšanas prasības atkarībā no finanšu vienības lieluma, darījumdarbības un riska profiliem: lai gan IKT rīku un sistēmu testēšana būtu jāveic visām vienībām, uz draudu vadītiem ielaušanās testiem (DVIT) balstīta padziļināta testēšana būtu obligāti jāveic tikai tām vienībām, ko kompetentās iestādes (balstoties uz šajā regulā noteiktajiem un EUI tālāk izstrādātajiem kritērijiem) ir atzinušas par nozīmīgām un kibergatavām. Ar šo regulu nosaka arī prasības testētājiem un DVIT rezultātu atzīšanai visā Savienībā attiecībā uz finanšu vienībām, kas darbojas vairākās dalībvalstīs.

Ar trešo personu saistītais IKT risks (25.–39. pants)

Regula ir izstrādāta tā, lai tā nodrošinātu ar trešo personu saistītā IKT riska stabilu uzraudzību. Šis mērķis tiks sasniegts, pirmkārt, ievērojot uz principiem balstītus noteikumus, ko piemēros finanšu vienību veiktajai trešo personu, kas sniedz IKT pakalpojumus, radītā riska uzraudzībai. Otrkārt, ar šo regulu tiek saskaņoti svarīgākie elementi pakalpojumos un attiecībās ar trešām personām, kas sniedz IKT pakalpojumus. Šie elementi aptver minimālos aspektus, kas atzīti par svarīgiem, lai finanšu vienība spētu pilnībā uzraudzīt ar trešo personu saistītu IKT risku visā tiesisko attiecību izveidošanas, izpildes, izbeigšanas, kā arī pēclīguma posmā.

Visbūtiskāk ir tas, ka līgumos, ko piemēro attiecībām, būs obligāti jāietver pilnīgs pakalpojumu apraksts, norāde par vietām, kur tiks veikta datu apstrāde, pilnīgs pakalpojumu līmeņa apraksts ar pievienotiem kvantitatīviem un kvalitatīviem darbības mērķiem, attiecīgi noteikumi par piekļūstamību, pieejamību, integritāti, drošību un personas datu aizsardzību, garantijas attiecībā uz piekļuves, atgūšanas un atgriešanās iespējām gadījumos, ja notikusi trešās personas, kas sniedz IKT pakalpojumus, atteice, trešām personām, kas sniedz IKT pakalpojumus, saistoši paziņošanas termiņi un ziņošanas pienākumi, finanšu vienības vai ieceltas trešās personas piekļuves, pārbaudes un revīzijas tiesības, skaidri noteiktas izbeigšanas tiesības un atsevišķas atkāpšanās stratēģijas. Turklāt, tā kā daļa no šiem līguma

noteikumiem var tikt standartizēti, ar regulu tiek sekmēta brīvprātīga līguma standartklauzulu izmantošana, kuras Komisija izstrādās attiecībā uz mākoņdatošanas pakalpojumu izmantošanu.

Visbeidzot, ar regulu tiek mēģināts sekmēt konverģenci attiecībā uz pieeju, kā uzraudzīt ar trešo personu saistīto IKT risku finanšu nozarē, pakļaujot kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, Savienības uzraudzības sistēmai. EUI, kas ir izraudzīta par katras šādas kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, galveno pārraugu, ar jaunu saskaņotu tiesisko regulējumu iegūst pilnvaras, lai nodrošinātu, ka tehnoloģiju pakalpojumu sniedzēji, kam ir kritiski svarīga loma finanšu nozares darbībā, tiek pienācīgi uzraudzīti visas Eiropas mērogā. Ar šo regulu paredzētā pārraudzības sistēma ir balstīta uz esošo finanšu pakalpojumu nozares institucionālo sistēmu, kurā EUI Apvienotā komiteja nodrošina starpnozaru koordināciju visos ar IKT risku saistītajos jautājumos saskaņā ar uzdevumiem, kas tai uzticēti attiecībā uz kiberdrošību, bet tai atbalstu sniedz attiecīgā apakškomiteja (Pārraudzības forums), kas veic sagatavošanās darbu individuālu lēmumu un kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, adresēto kolektīvo ieteikumu pieņemšanai.

Informācijas apmaiņa (40. pants)

Lai uzlabotu informētību par IKT risku, mazinātu tā izplatīšanos, atbalstītu finanšu vienību aizsardzības spējas un apdraudējumu atklāšanas paņēmienus, regula ļauj finanšu vienībām izveidot kārtību, kādā tās savstarpēji apmainās ar informāciju par kiberdraudiem un izlūkdatiem.

2020/0266 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA

par finanšu sektora digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014 un (ES) Nr. 909/2014

(Dokuments attiecas uz EEZ)

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 114. pantu,

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas dalībvalstu parlamentiem,

ņemot vērā Eiropas Centrālās bankas atzinumu[25],

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu[26],

saskaņā ar parasto likumdošanas procedūru,

tā kā:

(1) Informācijas un komunikācijas tehnoloģijas (IKT) digitālajā laikmetā atbalsta sarežģītas sistēmas, kas tiek lietotas ikdienas sabiedriskajām darbībām. Tās nodrošina mūsu ekonomikas darbību svarīgās nozarēs, ieskaitot finanšu nozari, un uzlabo vienotā tirgus darbību. Lielāka digitalizācija un savstarpēja savienojamība arī pastiprina IKT riskus, padarot sabiedrību kopumā un jo īpaši finanšu sistēmu neaizsargātāku pret kiberdraudiem vai IKT traucējumiem. Lai gan IKT sistēmu plašais lietojums, augstā digitalizācija un savienojamība mūsdienās ir visu Savienības finanšu vienību veikto darbību pamatiezīmes, to darbības pamatprincipos vēl nav pietiekami dziļi integrēta digitālā noturība.

(2) IKT izmantošana pēdējās desmitgadēs ir ieguvusi nozīmīgu lomu finanšu nozarē, un mūsdienās tā ir kļuvusi kritiski svarīga visu finanšu vienību parastajās ikdienas darbībās. Digitalizācija aptver, piemēram, maksājumus, kas arvien vairāk pāriet no skaidras naudas un papīra dokumentu izmantošanas uz digitāliem risinājumiem, kā arī vērtspapīru tīrvērti un norēķinus, elektronisko un algoritmisko tirdzniecību, aizdošanas un finansēšanas darbības, savstarpējo finansēšanu, kredītreitingu, apdrošināšanas saistību uzņemšanos, pretenziju apstrādi un biroja administratīvo darbu. Visa finanšu nozare ir kļuvusi lielākoties digitāla, turklāt digitalizācija ir arī padziļinājusi savstarpējos savienojumus un atkarības finanšu nozares iekšienē, kā arī attiecībās ar trešo personu infrastruktūru un to sniegtajiem pakalpojumiem.

(3) Eiropas Sistēmisko risku kolēģija (ESRK) 2020. gada ziņojumā par sistēmisko kiberrisku[27] ir atkārtoti uzsvērusi, kā finanšu vienību, finanšu tirgu un finanšu tirgus

[25] [*pievienot atsauci*] OV C , , . lpp.
[26] [*pievienot atsauci*] OV C , , . lpp.

infrastruktūras augstā savstarpējā savienojamība, jo īpaši to IKT sistēmu savstarpējā atkarība, varētu radīt sistēmisku neaizsargātību, jo vietēja mēroga kiberincidenti kādā no aptuveni 22 000 Savienības finanšu vienībām[28] varētu ātri izplatīties visā finanšu sistēmā, pāri valstu robežām. Smagi IKT pārkāpumi finanšu nozarē ietekmē ne tikai finanšu vienības atsevišķi. Tie arī atvieglo vietēja mēroga neaizsargātības izplatīšanos finanšu sakaru kanālos un, iespējams, var radīt nelabvēlīgas sekas Savienības finanšu sistēmas stabilitātei, izraisot likviditātes pazemināšanos un liekot zust vispārējai pārliecībai un uzticībai finanšu tirgiem.

(4) IKT riski pēdējos gados ir piesaistījuši valstu, Eiropas un starptautiskās politikas veidotāju, regulatoru un standartu noteikšanas struktūru uzmanību, liekot tām mēģināt uzlabot noturību, noteikt standartus, kā arī koordinēt regulējošo vai uzraudzības darbu. Starptautiskajā līmenī Bāzeles Banku uzraudzības komitejas, Maksājumu un tirgus infrastruktūru komitejas, Finanšu stabilitātes padomes, Finanšu stabilitātes institūta, kā arī G7 un G20 valstu grupu mērķis ir sniegt dažādu jurisdikciju kompetentajām iestādēm un tirgus dalībniekiem instrumentus finanšu sistēmu noturības stiprināšanai.

(5) Neraugoties uz mērķtiecīgu politiku un likumdošanas iniciatīvām valstu un Eiropas līmenī, IKT riski turpina sagādāt problēmas Savienības finanšu sistēmas darbības noturībai, veiktspējai un stabilitātei. Pēc 2008. gada finanšu krīzes īstenotā reforma galvenokārt stiprināja Savienības finanšu nozares finansiālo noturību un tika veikta ar mērķi aizsargāt Savienības konkurētspēju un stabilitāti no ekonomiskā, prudenciālā un tirgus darbības viedokļa. Lai gan IKT drošība un digitālā noturība ir daļa no operacionālā riska, tām pēckrīzes regulatoru darba programmā ir veltīta mazāka uzmanība, un tās ir attīstītas tikai dažās Savienības finanšu pakalpojumu politikas un regulējošās vides jomās vai dažās dalībvalstīs.

(6) Komisijas 2018. gada Finanšu tehnoloģijas rīcības plānā[29] tika uzsvērts, cik svarīgi ir padarīt Savienības finanšu nozari elastīgāku arī no darbības perspektīvas, lai nodrošinātu tās tehnoloģisko drošību un labu darbību, ātru atgūšanos no IKT pārkāpumiem un incidentiem, kas galu galā ļaus efektīvi un netraucēti sniegt finanšu pakalpojumus visā Savienībā, tostarp stresa situācijās, vienlaikus saglabājot patērētāju un tirgus uzticību un paļāvību.

(7) Eiropas Banku iestāde (EBI), Eiropas Vērtspapīru un tirgu iestāde (EVTI) un Eiropas Apdrošināšanas un aroda pensiju iestāde (EAAPI) (kopā sauktas par "Eiropas uzraudzības iestādēm" jeb "EUI") 2019. gada aprīlī kopīgi publicēja divus tehniskos ieteikumus, aicinot īstenot vienveidīgu pieeju IKT riskam finanšu nozarē un iesakot proporcionāli stiprināt finanšu pakalpojumu nozares digitālās darbības noturību ar Savienības specifisku nozares iniciatīvu.

---

27 ESRK 2020. gada februāra ziņojums par sistēmisko kiberrisku, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

28 Kā norādīts Eiropas uzraudzības iestāžu pārskatam pievienotajā ietekmes novērtējumā SWD(2017) 308, ir aptuveni 5665 kredītiestādes, 5934 ieguldījumu brokeru sabiedrības, 2666 apdrošināšanas sabiedrības, 1573 AKUI, 2500 ieguldījumu pārvaldības sabiedrības, 350 tirgus infrastruktūras (piemēram, *CCP*, biržas, sistemātiskie internalizētāji, darījumu reģistri un daudzpusējas tirdzniecības sistēmas), 45 *CRA* un 2500 pilnvarotas maksājumu iestādes un elektroniskās naudas iestādes. Kopā — aptuveni līdz 21 233 vienībām, neiekļaujot kolektīvās finansēšanas vienības, obligātos revidentus un revīzijas uzņēmumus, kriptoaktīvu pakalpojumu sniedzējus un etalonu administratorus.

29 Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Centrālajai Bankai, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai "*Finanšu tehnoloģijas rīcības plāns konkurētspējīgākam un inovatīvākam Eiropas finanšu sektoram"*, COM/2018/0109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.

(8) Savienības finanšu nozare tiek regulēta ar saskaņotu vienotu noteikumu kopumu, bet to pārvalda Eiropas finanšu uzraudzības sistēma. Neraugoties uz to, noteikumi, kas attiecas uz digitālās darbības noturību un IKT drošību, vēl nav pilnīgi vai konsekventi saskaņoti, lai gan digitālās darbības noturība digitālajā laikmetā ir ļoti svarīga finanšu stabilitātes un tirgus integritātes nodrošināšanai — ne mazāk svarīga, piemēram, par vienotiem prudenciālajiem vai tirgus rīcības standartiem. Tādēļ vienotais noteikumu kopums un uzraudzības sistēma būtu jāattīsta, lai aptvertu arī šo komponentu, paplašinot finanšu stabilitātes un tirgus integritātes uzraudzībai un aizsardzībai norīkoto finanšu uzraudzības iestāžu pilnvaras.

(9) Tiesību aktu nesakritības un nevienāda valstu regulatīvā vai uzraudzības pieeja attiecībā uz IKT risku rada šķēršļus izveidot finanšu pakalpojumu vienoto tirgu, apgrūtinot pārrobežu finanšu vienību brīvību veikt uzņēmējdarbību un sniegt pakalpojumus. Tāpat varētu tikt kropļota konkurence starp viena veida finanšu vienībām, kas darbojas dažādās dalībvalstīs. Īpaši jomās, kurās saskaņošana Savienības līmenī ir bijusi ļoti ierobežota, piemēram, digitālās darbības noturības testēšanā, vai tādas nav bijis, piemēram, ar trešo personu saistītā IKT riska uzraudzībā, atšķirības, kas izriet no paredzamās attīstības valstu līmenī, varētu radīt papildu šķēršļus vienotā tirgus darbībai, tādējādi kaitējot tirgus dalībniekiem un finanšu stabilitātei.

(10) Daļējais veids, kādā ar IKT risku saistītie noteikumi līdz šim ir risināti Savienības līmenī, liecina par nepilnībām vai pārklāšanos svarīgās jomās, piemēram, ar IKT saistītu incidentu paziņošanu un digitālās darbības noturības testēšanu, un rada pretrunas sakarā ar atšķirīgu valsts noteikumu rašanos vai tādu noteikumu neefektīvu piemērošanu izmaksu ziņā, kuri pārklājas. Tas jo īpaši nelabvēlīgi ietekmē tādu IKT ietilpīgu lietotāju kā finanšu nozari, jo tehnoloģiju riskiem nav robežu un finanšu nozare plaši izvieto pakalpojumus pāri robežām Savienībā un ārpus tās.

Individuālām finanšu vienībām, kuras darbojas pāri robežām vai kurām ir vairākas atļaujas (piem., vienai un tai pašai finanšu vienībai var būt banku darbības, ieguldījumu brokeru sabiedrības un maksājumu iestādes atļaujas, kuras izdevušas dažādas kompetentās iestādes vienā vai vairākās dalībvalstīs), ir grūti pašām saskanīgi un izmaksu ziņā efektīvi novērst IKT riskus un mazināt IKT incidentu nelabvēlīgo ietekmi.

(11) Tā kā vienotajam noteikumu kopumam nav pievienota visaptveroša IKT vai operacionālā riska sistēma, ir nepieciešams papildus saskaņot galvenās digitālās darbības noturības prasības visām finanšu vienībām. Spējas un kopējā noturība, ko finanšu vienības saskaņā ar galvenajām prasībām attīstītu, lai izturētu darbības pārtrauci, palīdzētu saglabāt Savienības finanšu tirgu stabilitāti un integritāti, tādējādi palīdzot nodrošināt Savienības ieguldītāju un patērētāju augsta līmeņa aizsardzību. Tā kā šīs regulas nolūks ir veicināt vienotā tirgus netraucētu darbību, tās pamatā vajadzētu būt LESD 114. pantam saskaņā ar tā interpretāciju Eiropas Savienības Tiesas pastāvīgajā judikatūrā.

(12) Regulas mērķis pirmkārt ir konsolidēt un uzlabot IKT riska prasības, kas līdz šim dažādās regulās un direktīvās ir skatītas atsevišķi. Lai gan šie Savienības tiesību akti aptvēra galvenās finanšu riska kategorijas (piem., kredītrisku, tirgus risku, darījuma partnera kredītrisku un likviditātes risku, tirgus uzvedības risku), ar tiem to pieņemšanas laikā nevarēja visaptveroši risināt visus darbības noturības komponentus. Šajos Savienības tiesību aktos sīkāk izstrādātās operacionālā riska prasības bieži vien deva priekšroku tradicionālajai kvantitatīvajai riska novēršanas pieejai (proti, nosakot

kapitāla prasību IKT riska segšanai), nevis paredzēja mērķtiecīgas kvalitatīvas prasības, ar kurām stiprināt spējas, nosakot prasības attiecībā uz aizsardzības, atklāšanas, ierobežošanas, seku novēršanas un izlabošanas spējām pēc incidentiem, kas saistīti ar IKT, vai nosakot ziņošanas un digitālās testēšanas spējas. Ar šīm direktīvām un regulām galvenokārt bija paredzēts aptvert būtiskākos prudenciālās uzraudzības, tirgus integritātes un uzvedības noteikumus.

Ar šo pasākumu, kas konsolidē un atjaunina noteikumus par IKT risku, visi noteikumi, kas attiecas uz digitālo risku finanšu nozarē, pirmo reizi tiktu konsekventi apvienoti vienā tiesību aktā. Tādējādi šai iniciatīvai būtu jānovērš nepilnības vai jāizlabo pretrunas dažos minētajos tiesību aktos, tostarp attiecībā uz tajos izmantoto terminoloģiju, un tai būtu skaidri jāatsaucas uz IKT risku, izmantojot mērķtiecīgus noteikumus par IKT riska pārvaldības iespējām, ziņošanu un testēšanu, kā arī ar trešo personu saistītā riska uzraudzību.

(13) Finanšu vienībām, risinot IKT risku, būtu jāievēro tāda pati pieeja un tādi paši uz principiem balstīti noteikumi. Konsekvence veicina uzticēšanos finanšu sistēmai un tās stabilitātes saglabāšanu, jo īpaši IKT sistēmu, platformu un infrastruktūru pārmērīgas izmantošanas laikā, kas rada lielāku digitālo risku.

Ievērojot kiberhigiēnas pamatus, būtu arī jāizvairās no augstu izmaksu rašanās tautsaimniecībai, samazinot IKT traucējumu ietekmi un izmaksas.

(14) Regulas izmantošana palīdz samazināt regulējuma sarežģītību, sekmē uzraudzības konverģenci, palielina juridisko noteiktību, vienlaikus veicinot atbilstības nodrošināšanas izmaksu ierobežošanu, jo īpaši attiecībā uz finanšu vienībām, kas darbojas pāri robežām, un mazinot konkurences kropļojumus. Tāpēc izvēle pieņemt regulu, lai izveidotu kopēju sistēmu finanšu vienību digitālās darbības noturībai, šķiet vispiemērotākais veids, kā nodrošināt viendabīgu un saskaņotu visu IKT riska pārvaldības komponentu piemērošanu Savienības finanšu nozarēs.

(15) Papildus finanšu pakalpojumu tiesību aktiem Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148[30] ir pašreizējais vispārējais kiberdrošības regulējums Savienības līmenī. No septiņām kritiski svarīgajām nozarēm minētā direktīva attiecas arī uz trim finanšu vienību veidiem, proti, kredītiestādēm, tirdzniecības vietām un centrālajiem darījumu partneriem. Tomēr, tā kā Direktīva (ES) 2016/1148 paredz mehānismu, kā valsts līmenī identificēt pamatpakalpojumu sniedzējus, praksē tās darbības jomā tiek iekļautas tikai dažas kredītiestādes, tirdzniecības vietas un centrālie darījumu partneri, ko noteikušas dalībvalstis un kam tādējādi tiek prasīts ievērot minētajā direktīvā noteiktās IKT drošības un incidentu paziņošanas prasības.

(16) Tā kā šī regula paaugstina digitālās noturības komponentu saskaņošanas līmeni, ieviešot prasības attiecībā uz IKT riska pārvaldību un ar IKT saistītu incidentu paziņošanu, kas ir stingrākas salīdzinājumā ar spēkā esošajos Savienības finanšu pakalpojumu tiesību aktos noteiktajām prasībām, tas nozīmē arī lielāku saskaņošanu salīdzinājumā ar Direktīvas (ES) 2016/1148 prasībām. Tādēļ šī regula attiecībā pret Direktīvu (ES) 2016/1148 ir *lex specialis*.

Ir svarīgi saglabāt stingru saikni starp finanšu nozari un Savienības horizontālo kiberdrošības regulējumu, kas nodrošinātu atbilstību dalībvalstu jau pieņemtajām

[30] 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.).

kiberdrošības stratēģijām un ļautu finanšu uzraudzības iestādēm apzināties kiberincidentus, kas ietekmē citas nozares, uz kurām attiecas Direktīva (ES) 2016/1148.

(17) Lai nodrošinātu starpnozaru mācību procesu un efektīvi izmantotu citu nozaru pieredzi, risinot kiberdraudus, Direktīvā (ES) 2016/1148 minētajām finanšu vienībām (piemēram, TID sadarbības grupai un *CSIRT*) vajadzētu būt daļai no minētās direktīvas "ekosistēmas".

EUI un valstu kompetentajām iestādēm attiecīgi vajadzētu būt iespējai piedalīties stratēģiskās politikas apspriedēs un TID sadarbības grupas tehniskajā darbā, attiecīgi apmainoties ar informāciju, un turpmāk sadarboties ar vienotajiem kontaktpunktiem, kas izraudzīti saskaņā ar Direktīvu (ES) 2016/1148. Kompetentajām iestādēm saskaņā ar šo regulu būtu jākonsultējas un jāsadarbojas ar valsts *CSIRT*, kas izraudzītas saskaņā ar Direktīvas (ES) 2016/1148 9. pantu.

(18) Svarīgi ir arī nodrošināt atbilstību Eiropas kritiskās infrastruktūras (EKI) direktīvai, kas pašlaik tiek pārskatīta, lai uzlabotu kritisko infrastruktūru aizsardzību un izturību pret draudiem, kas nav saistīti ar kiberuzbrukumiem, un tas varētu atstāt iespējamu ietekmi uz finanšu nozari[31].

(19) Mākoņdatošanas pakalpojumu sniedzēji ir viena no digitālo pakalpojumu sniedzēju kategorijām, uz ko attiecas Direktīva (ES) 2016/1148. Uz tiem attiecas *ex post* uzraudzība, ko veic valsts iestādes, kuras izraudzītas saskaņā ar minēto direktīvu, un kas attiecas tikai uz šajā aktā noteiktajām IKT drošības un incidentu paziņošanas prasībām. Tā kā ar šo regulu izveidotā pārraudzības sistēma attiecas uz visām kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, tostarp mākoņdatošanas pakalpojumu sniedzējiem, ja tie sniedz IKT pakalpojumus finanšu vienībām, būtu jāuzskata, ka tā papildina saskaņā ar Direktīvu (ES) 2016/1148 noteikošo uzraudzību. Turklāt ar šo regulu izveidotajai pārraudzības sistēmai būtu jāattiecas uz mākoņdatošanas pakalpojumu sniedzējiem, jo nav Savienības horizontālās nozarneitrālas sistēmas, ar ko izveidotu digitālo pārraudzības iestādi.

(20) Lai turpinātu pilnībā kontrolēt IKT riskus, finanšu vienībām ir jābūt visaptverošām spējām, kas nodrošina spēcīgu un efektīvu IKT riska pārvaldību, līdztekus īpašiem mehānismiem un rīcībpolitikai attiecībā uz ziņošanu par incidentiem, kas saistīti ar IKT, IKT sistēmu testēšanu, kontroli un procesiem, kā arī ar trešo personu saistītā IKT riska pārvaldību. Būtu jāpaaugstina finanšu sistēmas digitālās darbības noturības slieksnis, vienlaikus ļaujot samērīgi piemērot prasības finanšu vienībām, kuras ir mikrouzņēmumi saskaņā ar Komisijas Ieteikumā 2003/361/EK[32] lietoto definīciju.

(21) Ar IKT saistīto incidentu paziņošanas robežvērtības un taksonomija valstu līmenī ievērojami atšķiras. Lai gan, izmantojot attiecīgo darbu, ko saskaņā ar Direktīvu (ES) 2016/1148 ir paveikusi Eiropas Savienības Kiberdrošības aģentūra (*ENISA*)[33] un

---

31 Padomes Direktīva 2008/114/EK (2008. gada 8. decembris) par to, lai apzinātu un noteiktu Eiropas Kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību (OV L 345, 23.12.2008., 75. lpp.).

32 Komisijas Ieteikums (2003. gada 6. maijs) par mikrouzņēmumu, mazo un vidējo uzņēmumu definīciju (OV L 124, 20.5.2003., 36. lpp.).

33 *ENISA* Incidentu klasifikācijas atsauces taksonomija, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

TID sadarbības grupa finanšu vienībām, var radīt kopēju platformu, pārējām finanšu vienībām joprojām pastāv vai var rasties atšķirīgas pieejas attiecībā uz robežvērtībām un taksonomiju. Tas ietver vairākas prasības, kas finanšu vienībām jāievēro, jo īpaši, darbojoties vairākās Savienības jurisdikcijās un finanšu grupas ietvaros. Turklāt šīs atšķirības var kavēt turpmāku vienotu vai centralizētu Savienības mehānismu izveidi, kuri paātrina ziņošanas procesu un atbalsta ātru un vienmērīgu informācijas apmaiņu starp kompetentajām iestādēm, kas ir būtiski IKT risku novēršanai liela mēroga uzbrukumu gadījumā ar potenciāli sistēmiskām sekām.

(22) Lai kompetentās iestādes varētu pildīt savus uzraudzības uzdevumus, iegūstot pilnīgu pārskatu par to, kāda ir ar IKT saistīto incidentu būtība, biežums, nozīme un ietekme, un lai veicinātu informācijas apmaiņu starp attiecīgajām valsts iestādēm, tostarp tiesībaizsardzības iestādēm un noregulējuma iestādēm, ir jāparedz noteikumi, ar ko ar IKT saistīto incidentu paziņošanas kārtību papildina ar prasībām, kuru pašlaik trūkst finanšu apakšnozares tiesību aktos, un novērš visus pašreizējos pārklāšanās un dublēšanās gadījumus, lai mazinātu izmaksas. Tādēļ ir svarīgi saskaņot kārtību, kādā tiek ziņots par incidentiem, kas ir saistīti ar IKT, nosakot, ka visām finanšu vienībām ir jāsniedz ziņojumi tikai to kompetentajām iestādēm. Turklāt EUI būtu jāpilnvaro sīkāk noteikt ar IKT saistīto incidentu paziņošanas elementus, piemēram, taksonomiju, termiņus, datu kopas, veidnes un piemērojamās robežvērtības.

(23) Digitālās darbības noturības testēšanas prasības ir izstrādātas dažās finanšu apakšnozarēs vairākās nekoordinētās valstu sistēmās, atšķirīgi risinot vienas un tās pašas problēmas. Šādi pārrobežu finanšu vienībām tiek radīta izmaksu dublēšanās, kā arī tiek apgrūtināta rezultātu savstarpējā atzīšana. Līdz ar to nekoordinēta testēšana var sašķelt vienoto tirgu.

(24) Turklāt, ja testēšana nav obligāta, neaizsargātība paliek neatklāta, radot lielākus draudus finanšu vienībai un galu galā visas finanšu nozares stabilitātei un integritātei. Bez Savienības iejaukšanās digitālās darbības noturības testēšana arī turpmāk būtu fragmentāra un dažādas jurisdikcijas savstarpēji neatzītu testēšanas rezultātus. Turklāt, tā kā ir maz ticams, ka citas finanšu apakšnozares pieņemtu šādas shēmas nozīmīgā apmērā, tās zaudētu iespējamos ieguvumus, piemēram, neaizsargātības un risku atklāšanu, aizsardzības spēju un darbības nepārtrauktības testēšanu, kā arī klientu, piegādātāju un darījumu partneru lielāku uzticību. Lai novērstu šādu pārklāšanos, atšķirības un nepilnības, ir nepieciešams paredzēt noteikumus, kuru mērķis ir koordinēt finanšu vienību un kompetento iestāžu veikto testēšanu, tādējādi sekmējot nozīmīgu finanšu vienību padziļinātas testēšanas savstarpēju atzīšanu.

(25) Finanšu vienību paļaušanos uz IKT pakalpojumiem daļēji nosaka to nepieciešamība pielāgoties jaunai konkurētspējīgai digitālai globālai ekonomikai, celt darījumdarbības efektivitāti un apmierināt klientu pieprasījumu. Šīs paļaušanās būtība un apmērs pēdējo gadu laikā ir pastāvīgi attīstījušies, sekmējot finanšu starpniecības izmaksu samazināšanos, ļaujot paplašināties darījumdarbībai un panākt finanšu pakalpojumu izvietošanas mērogojamību, vienlaikus piedāvājot plašu IKT rīku klāstu sarežģītu iekšējo procesu pārvaldībai.

(26) Šo IKT pakalpojumu plašo izmantošanu apliecina sarežģītas līgumiskas vienošanās, kuru kontekstā finanšu vienībām bieži rodas grūtības vienoties par līguma noteikumiem, kas būtu pielāgoti piesardzības standartiem vai citām regulējošām prasībām, kuras tām jāievēro, vai citādi īstenot īpašas tiesības, piemēram, piekļuves tiesības vai revīzijas tiesības, ja vienošanās tādas paredz. Turklāt daudzos šādos līgumos nav paredzēti pietiekami aizsardzības pasākumi, kas ļautu pilnībā uzraudzīt

apakšuzņēmuma procesus, tādējādi liedzot finanšu vienībai spēju novērtēt šos saistītos riskus. Turklāt, tā kā trešās personas, kas ir IKT pakalpojumu sniedzējas, bieži sniedz standartizētus pakalpojumus dažādu veidu klientiem, šādi līgumi ne vienmēr pienācīgi apmierina finanšu nozares dalībnieku individuālās vai īpašās vajadzības.

(27) Neraugoties uz atsevišķiem vispārīgiem noteikumiem par ārpakalpojumiem, kas iekļauti Savienības tiesību aktos par finanšu pakalpojumiem, līgumiskās dimensijas uzraudzība Savienības tiesību aktos nav pilnībā nostiprināta. Tā kā nav skaidru un pielāgotu Savienības standartu, kas attiektos uz līgumisku vienošanos, kas ir noslēgta ar trešām personām, kas sniedz IKT pakalpojumus, IKT riska ārējais avots nav visaptveroši aplūkots. Tādēļ ir nepieciešams noteikt konkrētus pamatprincipus, pēc kuriem vadās finanšu vienības, veicot ar trešo personu saistītā IKT riska pārvaldību, papildinot tos ar līgumisko pamattiesību kopumu attiecībā uz vairākiem līgumu izpildes un izbeigšanas elementiem, lai nostiprinātu konkrētus minimālos aizsardzības pasākumus, kuri ir pamatā finanšu vienību spējai efektīvi uzraudzīt visus riskus, kuri rodas IKT trešās personas līmenī.

(28) Attiecībā uz IKT risku, kas saistīts ar trešo personu, un atkarību no trešās personas piedāvātajiem IKT pakalpojumiem trūkst viendabības un konverģences. Neraugoties uz atsevišķiem centieniem risināt īpašo ārpakalpojumu jomu, piemēram, 2017. gada ieteikumiem par mākoņpakalpojumu sniedzēju ārpakalpojumu izmantošanu[34], Savienības tiesību aktos gandrīz nav risināts jautājums par sistēmisko risku, ko varētu izraisīt finanšu nozares pakļautība ierobežotam skaitam kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus. Šo nepietiekamību Savienības līmenī saasina tas, ka nav īpaša pilnvarojuma un rīku, kas ļautu valstu uzraugiem gūt labu izpratni par atkarību no trešām personām, kas sniedz IKT pakalpojumus, un pienācīgi uzraudzīt risku, ko rada koncentrēta atkarība no trešām personām, kas sniedz IKT pakalpojumus.

(29) Ņemot vērā iespējamos sistēmiskos riskus, ko rada biežākas ārpakalpojumu izmantošanas prakse un IKT trešo personu koncentrācija, un paturot prātā to, ka nav pietiekamu valstu mehānismu, kas ļautu finanšu uzraudzības iestādēm kvantitatīvi noteikt, kvalificēt un novērst to IKT risku sekas, kuri rodas kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, ir nepieciešams izveidot atbilstīgu Savienības pārraudzības sistēmu, kas ļautu pastāvīgi uzraudzīt to trešo personu, kas sniedz IKT pakalpojumus, darbības, kuri ir kritiski svarīgi pakalpojumu sniedzēji finanšu vienībām.

(30) Tā kā IKT apdraudējumi kļūst sarežģītāki un attīstītāki, labi atklāšanas un profilakses pasākumi lielākoties ir atkarīgi no regulāras apdraudējumu un neaizsargātības izlūkdatu apmaiņas starp finanšu vienībām. Informācijas apmaiņa veicina lielāku informētību par kiberdraudiem, kas savukārt uzlabo finanšu vienību spēju novērst draudu pārtapšanu reālos incidentos un ļauj finanšu vienībām labāk ierobežot ar IKT saistīto incidentu ietekmi un efektīvāk novērst to sekas. Nepastāvot Savienības līmeņa norādījumiem, šādu izlūkdatu apmaiņu, šķiet, ir kavējuši vairāki faktori, jo īpaši nenoteiktība attiecībā uz saderību ar datu aizsardzības, pretmonopola un atbildības noteikumiem.

(31) Turklāt noderīga informācija tiek noklusēta tādēļ, ka pastāv šaubas par to, kādu informāciju var koplietot ar citiem tirgus dalībniekiem vai iestādēm, kas nav uzraudzības iestādes (piemēram, *ENISA* attiecībā uz analītiskajiem ievaddatiem vai

[34] Ieteikumi mākoņpakalpojumu izmantošanai (EBA/REC/2017/03), patlaban atcelti ar EBI Pamatnostādnēm par ārpakalpojumu izmantošanu (EBA/GL/2019/02).

Eiropolu — tiesībaizsardzības mērķiem). Informācijas apmaiņas apjoms un kvalitāte joprojām ir ierobežoti un sadrumstaloti, attiecīga apmaiņa pārsvarā tiek veikta vietējā līmenī (saskaņā ar valstu iniciatīvām), un nepastāv konsekventa Savienības mēroga informācijas apmaiņas kārtība, kas būtu pielāgota integrētas finanšu nozares vajadzībām.

(32) Tādēļ finanšu vienības būtu jāmudina kolektīvi izmantot to individuālās zināšanas un praktisko pieredzi stratēģiskā, taktiskā un darbības līmenī, lai uzlabotu to spējas pienācīgi novērtēt un uzraudzīt kiberdraudus, aizsargāties pret tiem un reaģēt uz tiem. Līdz ar to ir nepieciešams ļaut Savienības līmenī rasties mehānismiem, kuri paredz brīvprātīgu informācijas apmaiņas kārtību un kuri, veikti uzticamā vidē, palīdzēs finanšu kopienai novērst apdraudējumus un kolektīvi reaģēt uz tiem, ātri ierobežojot IKT risku izplatīšanos un kavējot iespējamu izplatīšanos pa finanšu kanāliem. Šie mehānismi būtu jāīsteno, pilnībā ievērojot piemērojamos Savienības konkurences tiesību noteikumus[35], kā arī tā, lai tiktu garantēta pilnīga Savienības datu aizsardzības noteikumu, galvenokārt Eiropas Parlamenta un Padomes Regulas (ES) 2016/679[36], ievērošana, jo īpaši saistībā ar minētās regulas 6. panta 1. punkta f) apakšpunktā minēto personas datu apstrādi, kas ir nepieciešama pārziņa vai trešās personas leģitīmo interešu ievērošanai.

(33) Neraugoties uz šajā regulā paredzēto plašo darbības jomu, piemērojot digitālās darbības noturības noteikumus, būtu jāņem vērā nozīmīgas atšķirības attiecībā uz finanšu vienību lielumu, darījumdarbības profilu vai pakļautību digitālajam riskam. Vispārīgs princips paredz, ka finanšu vienībām, novirzot resursus un spējas IKT riska pārvaldības sistēmas īstenošanai, ar IKT saistītās vajadzības ir pienācīgi jālīdzsvaro ar to lielumu un darījumdarbības profilu, savukārt kompetentajām iestādēm ir jāturpina vērtēt un pārskatīt šādas sadales pieeja.

(34) Tā kā lielākām finanšu vienībām varētu būt vairāk resursu un tās varētu ātri novirzīt līdzekļus pārvaldības struktūru attīstīšanai un dažādu korporatīvo stratēģiju izveidošanai, sarežģītāka pārvaldības kārtība būtu obligāti jāizveido tikai tām finanšu vienībām, kas nav mikrouzņēmumi šīs regulas izpratnē. Šādām vienībām ir lielākas iespējas izveidot īpašas vadības funkcijas, lai uzraudzītu nolīgumus ar trešām personām, kas sniedz IKT pakalpojumus, vai pārvarētu krīzi, organizētu IKT riska pārvaldību atbilstīgi trīs aizsardzības līniju modelim vai pieņemtu cilvēkresursu dokumentu, kurā visaptveroši būtu izskaidrota piekļuves tiesību rīcībpolitika.

Šo pašu apsvērumu dēļ tikai šādas finanšu vienības būtu jāaicina veikt padziļinātus novērtējumus pēc būtiskām tīklu un informācijas sistēmu infrastruktūras un procesu izmaiņām, regulāri veikt mantoto IKT sistēmu riska analīzi vai paplašināt darbības nepārtrauktības, reaģēšanas un seku novēršanas plānu testēšanu, lai aptvertu scenārijus, kuros notiek pārslēgšanās starp primāro IKT infrastruktūru un rezerves mehānismiem.

(35) Turklāt, tā kā draudu vadīti ielaušanās testi būtu obligāti jāveic tikai tām finanšu vienībām, kas identificētas kā nozīmīgas padziļinātās digitālās darbības noturības testēšanas mērķiem, ar šādu testu veikšanu saistītie administratīvie procesi un

---

35 Komisijas paziņojums "Pamatnostādnes par Līguma par Eiropas Savienības darbību 101. panta piemērojamību horizontālās sadarbības nolīgumiem", 2011/C 11/01.

36 Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

finansiālās izmaksas būtu jāsedz nelielam skaitam finanšu vienību. Visbeidzot, lai mazinātu regulatīvo slogu, tikai tām finanšu vienībām, kas nav mikrouzņēmumi, būtu jālūdz regulāri ziņot kompetentajām iestādēm par visām izmaksām un zaudējumiem, ko radījuši IKT traucējumi, un pēc būtiskiem IKT traucējumiem veiktās pēcincidentu pārskatīšanas rezultātiem.

(36) Lai nodrošinātu pilnīgu saskaņotību un kopējo vienveidību starp finanšu vienību darījumdarbības stratēģijām, no vienas puses, un IKT riska pārvaldības veikšanu, no otras puses, vadības struktūrai ir jāsaglabā nozīmīga un aktīva loma IKT riska pārvaldības sistēmas un kopējās digitālās darbības noturības stratēģijas vadībā un pielāgošanā. Vadības struktūras pieejai ir jābūt ne tikai vērstai uz to, kā nodrošināt IKT sistēmu noturību, bet arī jāaptver cilvēki un procesi, izmantojot rīcībpolitikas pasākumu kopumu, kas katrā korporatīvās vadības un personāla līmenī kultivē augstu informētību par kiberriskiem un apņemšanos visos līmeņos ievērot stingru kiberhigiēnu.

Vadības struktūras galīgajai atbildībai par finanšu vienības IKT risku pārvaldību ir jābūt šādas visaptverošas pieejas virsprincipam, kas tālāk izpaužas kā vadības struktūras pastāvīga iesaiste IKT riska pārvaldības uzraudzības kontrolē.

(37) Turklāt vadības struktūras pilnīga atbildība iet roku rokā ar tāda IKT ieguldījumu līmeņa un kopējā finanšu vienības budžeta nodrošināšanu, lai būtu iespējams sasniegt digitālās darbības noturības pamatscenāriju.

(38) Pamatojoties uz attiecīgiem starptautiskiem, nacionāliem un nozares noteiktiem standartiem, pamatnostādnēm, ieteikumiem vai pieejām kiberdraudu pārvaldībai[37], šī regula veicina funkciju kopumu, kas sekmē IKT riska pārvaldības vispārējo strukturēšanu. Ja galvenās spējas, ko ievieš finanšu vienības, apmierina šajā regulā noteikto funkciju (identifikācijas, aizsardzības un profilakses, atklāšanas, reaģēšanas un seku novēršanas, mācīšanās un attīstības, saziņas) mērķu vajadzības, finanšu vienības arī turpmāk varēs izmantot dažādi formulētus vai citā kategorijā iekļautus IKT riska pārvaldības modeļus.

(39) Lai neatpaliktu no strauji mainīgās kiberdraudu vides, finanšu vienībām būtu jāuztur atjauninātas IKT sistēmas, kas ir uzticamas un kam ir pieejama pietiekama jauda, lai ne tikai garantētu darbu veikšanai nepieciešamo datu apstrādi, bet arī nodrošinātu tehnoloģisko noturību, ļaujot finanšu vienībām pienācīgi tikt galā ar nepieciešamo papildu apstrādi, ko var radīt saspringti tirgus apstākļi vai citas nelabvēlīgas situācijas. Lai gan šī regula neparedz konkrētu IKT sistēmu, instrumentu vai tehnoloģiju standartizāciju, tā balstās uz Eiropas un starptautiski atzītu tehnisko standartu (piemēram, *ISO*) vai nozares labākās prakses piemērotu izmantošanu finanšu vienībās, ciktāl šāda izmantošana pilnībā atbilst īpašiem uzraudzības norādījumiem par starptautisko standartu izmantošanu un iekļaušanu.

(40) Ir nepieciešami efektīvi darbības nepārtrauktības un seku novēršanas plāni, lai finanšu vienības varētu nekavējoties un ātri atrisināt ar IKT saistītos incidentus, jo īpaši kiberuzbrukumus, ierobežojot kaitējumu un dodot priekšroku darbību atsākšanai un

---

[37] CPMI-IOSCO. *Guidance on cyber resilience for financial market infrastructures*, https://www.bis.org/cpmi/publ/d146.pdf G7 *Fundamental Elements of Cybersecurity for the Financial Sector*, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; *NIST* kiberdrošības regulējums, https://www.nist.gov/cyberframework; FSP *CIRR* rīku kopums, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document.

seku novēršanas darbībām. Tomēr, lai gan rezerves sistēmām apstrāde būtu jāsāk bez nepamatotas kavēšanās, šī uzsākšana nekādi nedrīkstētu apdraudēt tīklu un informācijas sistēmu integritāti un drošību vai datu konfidencialitāti.

(41) Lai gan šī regula ļauj finanšu vienībām elastīgi konstatēt mērķus attiecībā uz seku novēršanas termiņiem un līdz ar to noteikt šādus mērķus, pilnībā ņemot vērā attiecīgās funkcijas būtību un kritisko svarīgumu, kā arī jebkādas specifiskās darījumdarbības vajadzības, mērķu noteikšanas procesā būtu nepieciešams izvērtēt arī iespējamo kopējo ietekmi uz tirgus efektivitāti.

(42) Kiberuzbrukumu būtiskās sekas tiek pastiprinātas gadījumos, kad tie notiek finanšu nozarē — jomā, kam ir daudz lielāks risks kļūt par mērķi ļaunprātīgiem izplatītājiem, kuri vēlas gūt finansiālu labumu tieši līdzekļu izcelsmes vietā. Lai mazinātu šādus riskus un novērstu, ka IKT sistēmas zaudē integritāti vai kļūst nepieejamas, tiek piekļūts konfidenciāliem datiem vai nodarīts kaitējums fiziskajai IKT infrastruktūrai, būtu ievērojami jāuzlabo finanšu vienību ziņošana par būtiskiem ar IKT saistītiem incidentiem.

Ar IKT saistītu incidentu paziņošana attiecībā uz visām finanšu vienībām būtu jāsaskaņo, nosakot tām pienākumu ziņot tikai to kompetentajām iestādēm. Lai gan šī ziņošana attiektos uz visām finanšu vienībām, tai nebūtu vienādi jāskar tās visas, jo attiecīgās būtiskuma robežvērtības un termiņi būtu jāpielāgo tā, lai aptvertu vienīgi būtiskus ar IKT saistītus incidentus. Tieša ziņošana ļautu finanšu uzraudzības iestādēm piekļūt informācijai par incidentiem, kas saistīti ar IKT. Tomēr finanšu uzraudzības iestādēm šī informācija būtu jānodod ar finansēm nesaistītām publiskām iestādēm (TID kompetentajām iestādēm, valsts datu aizsardzības iestādēm un tiesībaizsardzības iestādēm, ja incidents ir bijis kriminăla rakstura). Informācijai par incidentiem, kas saistīti ar IKT, būtu jāplūst abpusēji: finanšu uzraudzības iestādēm būtu jāsniedz finanšu vienībai visa nepieciešamā atgriezeniskā saite vai norādījumi, savukārt EUI būtu jādalās ar anonimizētiem datiem par apdraudējumiem un neaizsargātību, kas saistīti ar notikumu, lai palīdzētu veidot kolektīvo aizsardzību plašākā nozīmē.

(43) Būtu jāparedz tālākas pārdomas par to, kā varētu centralizēt ar IKT saistīto incidentu paziņošanu, izmantojot vienotu centralizētu ES centrmezglu, kas vai nu tieši saņemtu attiecīgos ziņojumus un automātiski informētu valstu kompetentās iestādes, vai centralizētu valstu kompetento iestāžu pārsūtītos ziņojumus un pildītu koordinācijas funkciju. EUI būtu jānosaka pienākums, apspriežoties ar ECB un *ENISA*, līdz noteiktam datumam izstrādāt kopīgu ziņojumu, kurā būtu izvērtēta šāda centralizēta ES centrmezgla izveides iespējamība.

(44) Lai panāktu stabilu digitālās darbības noturību, kā arī ievērojot starptautiskos standartus (piemēram, G7 draudu vadītas ielaušanās testēšanas pamatelementus), finanšu vienībām būtu regulāri jātestē savu IKT sistēmu un personāla preventīvo, atklāšanas, reaģēšanas un seku novēršanas spēju efektivitāte, lai atklātu un risinātu potenciālo IKT neaizsargātību. Lai reaģētu uz finanšu apakšnozaru starpā un to iekšienē pastāvošajām atšķirībām saistībā ar finanšu vienību sagatavotību kiberdrošības jomā, testēšanā jāietver dažādi rīki un darbības, sākot no pamatprasību novērtēšanas (piemēram, neaizsargātības novērtējumi un skenēšana, atklātā pirmkoda analīze, tīkla drošības novērtējumi, nepilnību analīze, fiziskās drošības pārbaudes, anketas un skenēšanas programmatūras risinājumi, pirmkodu pārskatīšana (ja iespējams), uz scenārijiem balstīti testi, saderības testēšana, veiktspējas testēšana, testēšana "no gala līdz galam") līdz padziļinātai testēšanai (piem., DVIT tādām finanšu vienībām, kuru IKT sagatavotība ir pietiekama, lai tās varētu veikt šādus testus). Tādēļ

nozīmīgām finanšu vienībām (piem., lielām kredītiestādēm, biržām, centrālajiem vērtspapīru depozitārijiem, centrālajiem darījumu partneriem utt.) digitālās darbības noturības testēšanai būtu jābūt prasīgākai. Vienlaikus digitālās darbības noturības testēšanas nozīmei būtu jābūt lielākai arī dažās apakšnozarēs, kam ir svarīga sistēmiska loma (piem., maksājumi, banku darbība, tīrvērte un norēķini), bet mazākai — citās apakšnozarēs (piem., aktīvu pārvaldītāji, kredītreitingu aģentūras utt.). Pārrobežu finanšu vienībām, kas izmanto savu brīvību veikt uzņēmējdarbību vai sniegt pakalpojumus Savienībā, vajadzētu ievērot vienotu padziļinātas testēšanas prasību kopumu (piemēram, DVIT) savā piederības dalībvalstī, un šajā testā būtu jāiekļauj IKT infrastruktūra visās jurisdikcijās, kurās pārrobežu grupa darbojas Savienībā, tādējādi pieļaujot, ka pārrobežu grupām testēšanas izmaksas rodas tikai vienā jurisdikcijā.

(45) Lai nodrošinātu ar trešo personu saistītā IKT riska stabilu uzraudzību, ir nepieciešams paredzēt uz principiem balstītu noteikumu kopumu, lai vadītu finanšu vienību veikto tāda riska uzraudzību, kas rodas saistībā ar funkciju nodošanu ārpakalpojumā trešām personām, kas sniedz IKT pakalpojumus, un vispārīgāk — saistībā ar atkarību no trešām personām, kas sniedz IKT pakalpojumus.

(46) Finanšu vienībai nepārtraukti jābūt pilnībā atbildīgai par šajā regulā paredzēto pienākumu izpildi. Samērīga uzraudzība riskam, kurš rodas trešām personām, kas IKT pakalpojumus, būtu jāorganizē, pienācīgi ņemot vērā ar IKT saistītās atkarības mērogu, sarežģītību un nozīmi, to pakalpojumu, procesu vai funkciju kritiskumu vai svarīgumu, uz kuriem attiecas līgumiskas vienošanās, un galu galā attiecīgos gadījumos — pamatojoties uz rūpīgu novērtējumu par iespējamo ietekmi uz finanšu pakalpojumu nepārtrauktību un kvalitāti individuālajā un grupas līmenī.

(47) Šādā uzraudzībā būtu jāievēro stratēģiska pieeja ar trešo personu saistītajam IKT riskam, kas tiek formalizēta, finanšu vienības vadības struktūrai pieņemot īpašu stratēģiju, kas balstās visu šādu atkarību no trešām personām, kas sniedz IKT pakalpojumus, pastāvīgā izvērtēšanā. Lai uzlabotu uzraugu informētību par atkarību no trešām personām, kas sniedz IKT pakalpojumus, un papildus atbalstītu ar šo regulu izveidoto pārraudzības sistēmu, finanšu uzraudzības iestādēm būtu regulāri jāsaņem nozīmīga informācija no reģistriem un jāspēj *ad hoc* kārtībā pieprasīt izrakstus no tiem.

(48) Padziļinātai analīzei pirms līguma noslēgšanas vajadzētu būt līgumiskas vienošanās oficiālas noslēgšanas pamatā un jānotiek pirms tās, savukārt līgumu izbeigšana būtu jāizraisa vismaz tādu apstākļu kopumam, kas liecina par trešās personas, kas sniedz IKT pakalpojumus, nepilnībām.

(49) Lai risinātu ar trešo personu saistītā IKT koncentrācijas riska sistēmisko ietekmi, būtu jāsekmē līdzsvarots risinājums, izmantojot elastīgu un pakāpenisku pieeju, jo neelastīgas robežvērtības vai stingri ierobežojumi var kavēt darījumdarbības veikšanu un līgumslēgšanas brīvību. Finanšu vienībām būtu rūpīgi jāizvērtē līgumiskas vienošanās, lai noteiktu šāda riska rašanās iespējamību, tostarp veicot padziļinātu analīzi par ārpakalpojumu tālākas deleģēšanas līgumiem, jo īpaši, ja tie noslēgti ar trešā valstī reģistrētām trešām personām, kas sniedz IKT pakalpojumus. Šajā posmā un nolūkā panākt taisnīgu līdzsvaru starp līgumu slēgšanas brīvības saglabāšanu un finanšu stabilitātes garantēšanu nav lietderīgi paredzēt stingras robežvērtības un ierobežojumus pakļautībai ar trešo personu saistītam IKT riskam. EUI, kas izraudzīta veikt pārraudzību attiecībā uz katru kritiski svarīgo trešo personu, kas sniedz IKT pakalpojumus (“galvenais pārraugs”), pildot pārraudzības uzdevumus, īpašu uzmanību

pievērš tam, lai pilnībā aptvertu savstarpējo atkarību apjomu un atklātu konkrētus gadījumus, kad kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, augsta koncentrācija Savienībā varētu radīt spiedienu uz Savienības finanšu sistēmas stabilitāti un integritāti, un tā vietā būtu jānodrošina dialogs ar kritiski svarīgajām trešām personām, kas sniedz IKT pakalpojumus, ja šāds risks ir identificēts[38].

(50) Lai varētu izvērtēt un regulāri uzraudzīt trešās personas, kas sniedz IKT pakalpojumus, spēju droši sniegt pakalpojumus finanšu vienībai, nelabvēlīgi neietekmējot tās noturību, ir jāsaskaņo galvenie līgumiskie elementi visā ar trešām personām, kas sniedz IKT pakalpojumus, noslēgto līgumu izpildes laikā. Šie elementi aptver tikai minimālos līgumiskos aspektus, kas tiek uzskatīti par svarīgiem, lai ļautu finanšu vienībai pilnībā uzraudzīt to, kā tiek nodrošināta tās digitālās darbības noturība, kas ir atkarīga no IKT pakalpojuma stabilitātes un drošības.

(51) Ar līgumisku vienošanos jo īpaši būtu jānosaka visu funkciju un pakalpojumu pilnīgs apraksts, funkciju sniegšanas un datu apstrādes vieta, kā arī jānorāda pilni pakalpojumu līmeņa apraksti, kam pievienoti kvantitatīvi un kvalitatīvi darbības mērķi atbilstīgi nolīgtajiem pakalpojumu līmeņiem, kas ļauj finanšu vienībai efektīvi veikt uzraudzību. Attiecībā uz finanšu vienības spēju nodrošināt ar trešo personu saistītā riska uzraudzību par būtiskiem elementiem tāpat būtu jāuzskata noteikumi par piekļūstamību, pieejamību, integritāti, drošību un personas datu aizsardzību, kā arī garantijas attiecībā uz piekļuvi, atgūšanu un atgriešanu trešās personas, kas sniedz IKT pakalpojumus, maksātnespējas, noregulējuma vai darījumdarbības izbeigšanas gadījumā.

(52) Lai nodrošinātu, ka finanšu vienības turpina pilnībā kontrolēt visu notikumu attīstību, kas varētu ietekmēt to IKT drošību, ir jānosaka trešās personas, kas sniedz IKT pakalpojumus, saistoši paziņošanas termiņi un ziņošanas pienākumi, ja iestājušies notikumi, kas varētu būtiski ietekmēt trešās personas, kas sniedz IKT pakalpojumus, spēju efektīvi veikt kritiski svarīgas vai svarīgas funkcijas, ieskaitot tā sniegtu palīdzību ar IKT saistīta incidenta gadījumā bez papildu maksas vai par iepriekš noteiktu maksu.

(53) Finanšu vienības vai tās ieceltas trešās personas piekļuves, pārbaudes un revīzijas tiesības ir svarīgi rīki finanšu vienības veiktās trešās personas, kas sniedz IKT pakalpojumus, darbības rezultātu pastāvīgās uzraudzības procesā, ko papildina tā pilnīga sadarbība pārbaužu laikā. Arī finanšu vienības kompetentajai iestādei būtu jābūt šādām tiesībām ar iepriekšēju paziņojumu pārbaudīt trešās personas, kas sniedz IKT pakalpojumus, un veikt tā revīziju, ievērojot konfidencialitāti.

(54) Ar līgumisku vienošanos būtu jāparedz skaidri noteiktas izbeigšanas tiesības un ar tām saistīti minimālie paziņošanas termiņi, kā arī atsevišķas atkāpšanās stratēģijas, kas jo īpaši ļauj noteikt obligātus pārejas periodus, kuros trešās personas, kas sniedz IKT pakalpojumus, turpina nodrošināt attiecīgās funkcijas ar mērķi mazināt traucējumu risku finanšu vienības līmenī vai ļauj tai efektīvi pāriet pie citas trešās personas, kas sniedz IKT pakalpojumus, vai arī izmantot uz vietas nodrošinātus risinājumus atbilstīgi sniegtā pakalpojuma sarežģītībai.

[38] Turklāt, ja rastos risks, ka dominējošā stāvoklī esoša trešā persona, kas sniedz IKT pakalpojumus, varētu to izmantot ļaunprātīgi, finanšu vienībām vajadzētu būt iespējai arī iesniegt oficiālu vai neoficiālu sūdzību Eiropas Komisijai vai valstu konkurences tiesību iestādēm.

(55) Turklāt, brīvprātīgi izmantojot līguma standartklauzulas, kuras Komisija izstrādājusi attiecībā uz mākoņdatošanas pakalpojumu izmantošanu, var nodrošināt papildu drošību finanšu vienībām un to trešām personām, kas sniedz IKT pakalpojumus, uzlabojot juridisko noteiktību attiecībā uz mākoņdatošanas pakalpojumu izmantošanu finanšu nozarē un to pilnībā saskaņojot ar Finanšu pakalpojumu regulas prasībām un gaidām. Šis darbs balstās uz pasākumiem, kas tika paredzēti jau 2018. gada Finanšu tehnoloģijas rīcības plānā, kurā tika izziņots Komisijas nodoms atbalstīt un veicināt līgumu standartklauzulu izstrādi finanšu vienību darbību uzticēšanai ārējiem mākoņdatošanas pakalpojumu sniedzējiem, par pamatu izmantojot starpnozaru mākoņdatošanas pakalpojumu jomas ieinteresēto personu centienus, ko Komisija ar finanšu nozares iesaisti ir veicinājusi.

(56) Lai veicinātu konverģenci un efektivitāti attiecībā uz uzraudzības pieejām ar trešo personu saistītajam IKT riskam finanšu nozarē, stiprinātu to finanšu vienību digitālās darbības noturību, kuras darbības funkciju veikšanā paļaujas uz kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, un tādējādi palīdzētu saglabāt Savienības finanšu sistēmas stabilitāti un finanšu pakalpojumu vienotā tirgus integritāti, kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, būtu jāpiemēro Savienības pārraudzības sistēma.

(57) Tā kā tikai pret kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, ir nepieciešama īpaša attieksme, būtu jāievieš izraudzīšanās mehānisms Savienības pārraudzības sistēmas piemērošanai, lai ņemtu vērā, kādā apmērā un veidā finanšu nozare paļaujas uz šādām trešām personām, kas sniedz IKT pakalpojumus, un uz tā pamata būtu jāveido kvantitatīvu un kvalitatīvu kritēriju kopums, kas noteiktu svarīguma parametrus kā pamatu pakļaušanai pārraudzībai. Kritiski svarīgajām trešām personām, kas sniedz IKT pakalpojumus, kas netiek automātiski izraudzīti, piemērojot minētos kritērijus, vajadzētu būt iespējai brīvprātīgi pievienoties pārraudzības sistēmai, savukārt tās trešās personas, kas sniedz IKT pakalpojumus, uz kurām jau attiecas Eirosistēmas līmenī izveidotie pārraudzības mehānismi, kuru mērķis ir atbalstīt Līguma par Eiropas Savienības darbību 127. panta 2. punktā minētos uzdevumus, attiecīgi būtu jāatbrīvo.

(58) Prasība, ka kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, jābūt juridiski nodibinātiem Savienībā, neparedz datu lokalizāciju, jo šī regula neparedz nekādas papildu prasības attiecībā uz datu uzglabāšanas vai apstrādes veikšanu Savienībā.

(59) Šim regulējumam nevajadzētu skart dalībvalstu kompetenci veikt savus pārraudzības uzdevumus attiecībā uz trešām personām, kas sniedz IKT pakalpojumus, kuri nav kritiski svarīgi saskaņā ar šo regulu, bet kurus var uzskatīt par svarīgiem valsts līmenī.

(60) Lai izmantotu finanšu pakalpojumu jomas pašreizējo daudzslāņaino institucionālo struktūru, EUI Apvienotajai komitejai būtu jāturpina nodrošināt vispārēju starpnozaru koordināciju attiecībā uz visiem ar IKT risku saistītajiem jautājumiem saskaņā ar tās uzdevumiem kiberdrošības jomā, un tā jāatbalsta jaunai apakškomitejai (Pārraudzības forumam), kas veic sagatavošanās darbus gan attiecībā uz atsevišķām kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, adresētiem lēmumiem, gan kolektīviem ieteikumiem, jo īpaši par kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, pārraudzības programmu salīdzinošo novērtēšanu un IKT koncentrācijas riska jautājumu risināšanas labākās prakses noteikšanu.

(61) Lai nodrošinātu, ka trešās personas, kas sniedz IKT pakalpojumus, kam ir kritiski svarīga loma finanšu nozares darbībā, ir samērīgi pārraudzīti Savienības mērogā, viena

no EUI būtu jāizraugās par katras kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, galveno pārraugu.

(62) Galvenajiem pārraugiem vajadzētu būt vajadzīgajām pilnvarām veikt kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, izmeklēšanu un pārbaudes uz vietas un neklātienē, piekļūt visām attiecīgajām telpām un atrašanās vietām un iegūt pilnīgu un atjauninātu informāciju, lai tie varētu iegūt patiesu priekšstatu par finanšu vienībām un Savienības finanšu sistēmai radīto, ar trešo personu saistīto IKT risku pēc tā veida, apmēra un ietekmes.

Galvenās pārraudzības uzticēšana EUI ir priekšnoteikums, lai novērtētu un risinātu IKT riska sistēmisko dimensiju finanšu jomā. Kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, ietekme Savienības mērogā un ar to saistītie iespējamie IKT koncentrācijas riska jautājumi mudina izvēlēties kolektīvu pieeju, kas tiek īstenota Savienības līmenī. Vairākkārtēju revīziju un piekļuves tiesību īstenošana, ko nošķirti veic daudzas kompetentās iestādes, koordinējot centienus maz vai nemaz, neradītu pilnīgu pārskatu par IKT risku, kas saistīts ar trešo personu, vienlaikus radot nevajadzīgu dublēšanos, slogu un sarežģītību kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, kuri saskaras ar šādiem daudziem pieprasījumiem.

(63) Turklāt galvenajiem pārraugiem būtu jāspēj sniegt ieteikumus par IKT riska jautājumiem un piemērotiem novēršanas pasākumiem, ieskaitot iebildumus pret konkrētu līgumisku vienošanos, kas ietekmē finanšu vienības vai finanšu sistēmas stabilitāti. Valstu kompetentajām iestādēm kā daļa no finanšu vienību prudenciālās uzraudzības funkcijas būtu pienācīgi jāņem vērā galveno pārraugu sniegto būtisko ieteikumu ievērošana.

(64) Pārraudzības sistēma neaizstāj, kā arī nekādā veidā un daļā neaizvieto finanšu vienību veikto tāda riska pārvaldību, ko rada trešo personu, kas sniedz IKT pakalpojumus, izmantošana, tostarp pienākumu pastāvīgi uzraudzīt līgumiskas vienošanās, kas noslēgtas ar kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, un neietekmē finanšu vienību pilnu atbildību par visu no šīs regulas un attiecīgajiem finanšu pakalpojumu tiesību aktiem izrietošo prasību ievērošanu un to izpildi. Lai izvairītos no dublēšanās un pārklāšanās, kompetentajām iestādēm būtu jāatturas individuāli veikt pasākumus, kuru mērķis ir uzraudzīt kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, riskus. Jebkurš šāds pasākums iepriekš būtu jākoordinē un par to jāvienojas saistībā ar pārraudzības sistēmu.

(65) Lai starptautiskā līmenī veicinātu konverģenci attiecībā uz labāko praksi, ko izmanto, pārskatot trešo personu, kas sniedz IKT pakalpojumus, digitālo riska pārvaldību, EUI būtu jāmudina noslēgt sadarbības nolīgumus ar attiecīgajām uzraudzības un regulatīvajām trešo valstu kompetentajām iestādēm, lai veicinātu ar trešo personu saistītā IKT riska novēršanas labākās prakses izstrādi.

(66) Lai apkopotu kompetento iestāžu ekspertu tehniskās zināšanas par operacionālā un IKT riska pārvaldību, galvenajiem pārraugiem būtu jāizmanto valstu uzraudzības pieredze un jāizveido īpašas pārbaudes grupas katrai atsevišķai kritiski svarīgai trešai personai, kas sniedz IKT pakalpojumus, apvienojot daudznozaru grupas, lai tās atbalstītu gan pārraudzības pasākumu sagatavošanu, gan faktisko izpildi, tostarp kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, pārbaudes uz vietas, kā arī pēc tam veicot vajadzīgos turpmākos pasākumus.

(67) Kompetentajām iestādēm jābūt visām nepieciešamajām uzraudzības, izmeklēšanas un sankciju pilnvarām, lai nodrošinātu šīs regulas piemērošanu. Administratīvie sodi

principā būtu jāpublicē. Tā kā finanšu vienības un trešās personas, kas sniedz IKT pakalpojumus, var būt nodibināti dažādās dalībvalstīs un tos var uzraudzīt dažādas nozares kompetentās iestādes, būtu jānodrošina cieša sadarbība starp attiecīgajām kompetentajām iestādēm, tostarp ar ECB attiecībā uz īpašiem uzdevumiem, ko tai uztic saskaņā ar Padomes Regulu (ES) Nr. 1024/2013[39], un ar EUI, veicot savstarpēju informācijas apmaiņu un sniedzot palīdzību saistībā ar uzraudzības darbībām.

(68) Lai turpinātu kvantitatīvi un kvalitatīvi raksturot kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, izraudzīšanās kritērijus un saskaņotu pārraudzības maksas, Komisijai būtu jādeleģē pilnvaras pieņemt aktus saskaņā ar Līguma par Eiropas Savienības darbību 290. pantu attiecībā uz: tādas sistēmiskas ietekmes tālāku precizēšanu, ko trešās personas, kas sniedz IKT pakalpojumus, darbība varētu radīt finanšu vienībām, kuras tas apkalpo, globālo sistēmiski nozīmīgo iestāžu (G-SNI) vai citu sistēmiski nozīmīgu iestāžu (C-SNI), kas paļaujas uz attiecīgo trešo personu, kas sniedz IKT pakalpojumus, skaitu, aktīvu trešo personu, kas sniedz IKT pakalpojumus, skaitu konkrētā tirgū, izmaksām, kas saistītas ar pāriešanu pie citas trešās personas, kas sniedz IKT pakalpojumus, to dalībvalstu skaitu, kurās darbojas attiecīgā trešā persona, kas sniedz IKT pakalpojumus, un kurās darbojas finanšu vienības, kas izmanto attiecīgo trešo personu, kas sniedz IKT pakalpojumus, kā arī pārraudzības maksu apmēru un to, kādā veidā tās ir jāmaksā.

Ir īpaši būtiski, lai Komisija, veicot sagatavošanas darbus, rīkotu atbilstīgas apspriešanās, tostarp ekspertu līmenī, un lai minētās apspriešanās tiktu rīkotas saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu[40]. Jo īpaši, lai deleģēto aktu sagatavošanā nodrošinātu vienādu dalību, Eiropas Parlaments un Padome visus dokumentus saņem vienlaicīgi ar dalībvalstu ekspertiem, un minēto iestāžu ekspertiem ir sistemātiska piekļuve Komisijas ekspertu grupu sanāksmēm, kurās notiek deleģēto aktu sagatavošana.

(69) Tā kā šī regula kopā ar Eiropas Parlamenta un Padomes Direktīvu (ES) Nr. 20xx/xx[41] paredz konsolidēt IKT riska pārvaldības noteikumus, kas ir iekļauti vairākās Savienības finanšu pakalpojumu jomas *acquis* regulās un direktīvās, tostarp Regulā (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014 un (ES) Nr. 909/2014, lai nodrošinātu pilnīgu konsekvenci, šīs regulas būtu jāgroza, lai precizētu, ka šajā regulā ir paredzēti attiecīgie ar IKT risku saistītie noteikumi.

Tehniskajiem standartiem būtu jānodrošina šajā regulā noteikto prasību konsekventa saskaņošana. EUI kā struktūras, kam ir ļoti specializētas zināšanas, būtu jāpilnvaro izstrādāt un iesniegt Komisijai ar politikas izvēlēm nesaistītu regulatīvu tehnisko standartu projektus. Būtu jāizstrādā regulatīvie tehniskie standarti tādās jomās kā IKT riska pārvaldība, ziņošana, testēšana un galvenās prasības ar trešo personu saistīta IKT riska stabilai uzraudzībai.

(70) Ir īpaši būtiski, lai Komisija, veicot sagatavošanās darbus, rīkotu atbilstīgu apspriešanos, tostarp ekspertu līmenī. Komisijai un EUI būtu jānodrošina, lai visas finanšu vienības varētu piemērot minētos standartus un prasības tā, lai piemērošana būtu samērīga ar minēto vienību darbības veidu, mērogu un sarežģītību.

---

39 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).

40 OV L 123, 12.5.2016., 1. lpp.

41 [*Lūdzu, ievietojiet pilnu atsauci*].

(71) Lai atvieglotu ar IKT saistītu būtisku incidentu ziņojumu salīdzināmību un nodrošinātu pārredzamību attiecībā uz līgumisku vienošanos par tādu IKT pakalpojumu izmantošanu, ko sniedz trešās personas, kas sniedz IKT pakalpojumus, EUI būtu jāpilnvaro izstrādāt īstenošanas tehnisko standartu projektus, ar kuriem izveido standartizētas veidnes, veidlapas un procedūras finanšu vienībām, lai ziņotu par būtiskiem ar IKT saistītiem incidentiem, kā arī standartizētas veidnes informācijas reģistram. Izstrādājot šos standartus, EUI jāņem vērā finanšu vienību lielums un sarežģītība, kā arī to darbības veida būtība un riska līmenis. Komisija būtu jāpilnvaro pieņemt šādus īstenošanas tehniskos standartus, pieņemot īstenošanas aktus saskaņā ar LESD 291. pantu un attiecīgi saskaņā ar Regulas (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010 15. pantu. Tā kā papildu prasības jau ir noteiktas ar deleģētiem un īstenošanas aktiem, kuru pamatā ir attiecīgi Regulās (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014 un (ES) Nr. 909/2014 paredzētie tehniskie normatīvie un īstenošanas tehniskie standarti, ir lietderīgi pilnvarot EUI individuāli vai kopīgi ar Apvienotās komitejas starpniecību iesniegt Komisijai regulatīvos un īstenošanas tehniskos standartus, lai pieņemtu deleģētos un īstenošanas aktus, ar kuriem īsteno un atjaunina esošos IKT riska pārvaldības noteikumus.

(72) Šis uzdevums būs saistīts ar spēkā esošo deleģēto un īstenošanas aktu, kas pieņemti dažādās finanšu pakalpojumu tiesību aktu jomās, vēlāku grozīšanu. Būtu jāgroza darbības joma pantiem par operacionālo risku, uz kuru pamata ar minētajiem aktiem ir piešķirtas pilnvaras pieņemt deleģētos un īstenošanas aktus, lai šajā regulā iekļautu visus noteikumus, kas attiecas uz digitālās darbības noturību un kas pašlaik ir minēto regulu sastāvdaļa.

(73) Ņemot vērā to, ka šīs regulas mērķi — proti, visām finanšu vienībām piemērojama augsta digitālās darbības noturības līmeņa sasniegšanu — nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, jo ir jāsaskaņo liels daudzums atšķirīgu noteikumu, kas šobrīd pastāv vai nu atsevišķos Savienības aktos, vai dažādu dalībvalstu tiesību sistēmās, bet tā mēroga un iedarbības dēļ minēto mērķi var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar Līguma par Eiropas Savienību 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā regulā paredz vienīgi tos pasākumus, kas ir vajadzīgi šā mērķa sasniegšanai,

IR PIEŅĒMUŠI ŠO REGULU.

I NODAĻA

VISPĀRĪGI NOSACĪJUMI

1. pants

Priekšmets

1. Šajā regulā ir noteiktas šādas vienotas prasības attiecībā uz tādu tīklu un informācijas sistēmu drošību, kas atbalsta finanšu vienību darījumdarbības procesus, kuri nepieciešami augsta kopējā digitālās darbības noturības līmeņa sasniegšanai:

   (a) finanšu vienībām piemērojamās prasības attiecībā uz:

   – informācijas un komunikācijas tehnoloģiju (IKT) riska pārvaldību;

   – ziņošanu kompetentajām iestādēm par būtiskiem ar IKT saistītiem incidentiem;

– digitālās darbības noturības testēšanu;

– ar kiberdraudiem un neaizsargātību saistītu informācijas un izlūkdatu apmaiņu;

– pasākumiem, ar kuriem finanšu vienības stabili pārvalda ar trešām personām saistīto IKT risku;

(b) prasības attiecībā uz līgumisku vienošanos, kas noslēgta starp trešām personām, kas sniedz IKT pakalpojumus, un finanšu vienībām;

(c) to trešo personu pārraudzības sistēma, kas sniedz kritiski svarīgus IKT pakalpojumus, gadījumiem, kad tās sniedz pakalpojumus finanšu vienībām;

(d) kompetento iestāžu sadarbības noteikumi un kompetento iestāžu uzraudzības un izpildes noteikumi attiecībā uz visiem jautājumiem, uz kuriem attiecas šī regula.

2. Attiecībā uz finanšu vienībām, kas noteiktas kā pamatpakalpojumu sniedzēji saskaņā ar valsts noteikumiem, ar kuriem transponē Direktīvas (ES) 2016/1148 5. pantu, šo regulu skata kā uz konkrētu nozari attiecināmu Savienības tiesību aktu minētās direktīvas 1. panta 7. punkta nozīmē.

2. pants

Darbības joma attiecībā uz personām

1. Šo regulu piemēro šādām vienībām:

(e) kredītiestādēm;

(f) maksājumu iestādēm;

(g) elektroniskās naudas iestādēm;

(h) ieguldījumu brokeru sabiedrībām;

(i) kriptoaktīvu pakalpojumu sniedzējiem, kriptoaktīvu emitentiem, aktīviem piesaistītu tokenu emitentiem un nozīmīgu aktīviem piesaistītu tokenu emitentiem;

(j) centrālajiem vērtspapīru depozitārijiem;

(k) centrālajiem darījumu partneriem;

(l) tirdzniecības vietām;

(m) darījumu reģistriem;

(n) alternatīvo ieguldījumu fondu pārvaldniekiem;

(o) pārvaldības sabiedrībām;

(p) datu ziņošanas pakalpojumu sniedzējiem;

(q) apdrošināšanas un pārapdrošināšanas sabiedrībām;

(r) apdrošināšanas starpniekiem, pārapdrošināšanas starpniekiem un apdrošināšanas papildpakalpojuma starpniekiem;

(s) arodpensiju iestādēm;

(t) kredītreitingu aģentūrām;

(u) obligātajiem revidentiem un revīzijas uzņēmumiem;

(v) kritiski svarīgu etalonu administratoriem;

(w) kolektīvās finansēšanas pakalpojumu sniedzējiem;

(x) vērtspapīrošanas repozitorijiem;

(y) trešām personām, kas sniedz IKT pakalpojumus.

2. Šā panta 1. punkta a)–t) apakšpunktā minētās vienības šajā regulā kopā sauc par "finanšu vienībām".

3. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

(1) "digitālās darbības noturība" ir finanšu vienības spēja veidot, nodrošināt un pārskatīt savu darbības integritāti no tehnoloģiskā viedokļa, tieši vai netieši, izmantojot IKT pakalpojumus, ko sniedz trešās personas, nodrošinot visas ar IKT saistītās iespējas, kas vajadzīgas, lai risinātu finanšu vienības izmantoto tīklu un informācijas sistēmu drošību, un kas atbalsta finanšu pakalpojumu nepārtrauktu sniegšanu un to kvalitāti;

(2) "tīklu un informācijas sistēma" ir tīklu un informācijas sistēma, kā definēts Direktīvas (ES) 2016/1148 4. panta 1. punktā;

(3) "tīklu un informācijas sistēmu drošība" ir tīklu un informācijas sistēmu drošība, kā definēts Direktīvas (ES) 2016/1148 4. panta 2. punktā;

(4) "IKT risks" ir jebkāds ar tīklu un informācijas sistēmu izmantošanu saistīts un saprātīgi identificējams apstāklis, tostarp nepareiza darbība, jaudas pārsniegšana, atteice, traucējums, kaitējums, ļaunprātīga izmantošana, zudums vai cita veida ļaunprātīga vai neļaunprātīga darbība, kas īstenošanās gadījumā varētu apdraudēt tīklu un informācijas sistēmu, jebkura tehnoloģiski atkarīga rīka vai procesa, darbības un noritošo procesu vai pakalpojumu sniegšanas drošību, tādējādi apdraudot datu, programmatūras vai cita IKT pakalpojumu un infrastruktūras komponenta integritāti vai pieejamību vai izraisot konfidencialitātes pārkāpumu, fiziskās IKT infrastruktūras bojājumu vai citu kaitīgu ietekmi;

(5) "informācijas aktīvs" ir materiāls vai nemateriāls informācijas kopums, ko ir vērts aizsargāt;

(6) "ar IKT saistīts incidents" ir neparedzēts identificēts notikums tīklu un informācijas sistēmās, kas izriet vai neizriet no ļaunprātīgas darbības, apdraud tīklu un informācijas sistēmu vai šādās sistēmās apstrādātās, glabātās vai pārraidītās informācijas drošību vai negatīvi ietekmē finanšu vienības sniegto finanšu pakalpojumu pieejamību, konfidencialitāti, nepārtrauktību vai autentiskumu;

(7) "būtisks ar IKT saistīts incidents" ir ar IKT saistīts incidents ar iespējamu lielu nelabvēlīgu ietekmi uz tīklu un informācijas sistēmām, kas atbalsta finanšu vienības kritiski svarīgas funkcijas;

(8) "kiberdraudi" ir kiberdraudi, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) 2019/881[42] 2. panta 8. punktā;

[42] Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (OV L 151, 7.6.2019., 15. lpp.).

(9) “kiberuzbrukums” ir ļaunprātīgs ar IKT saistīts incidents, ar ko tiek mēģināts iznīcināt, pakļaut, mainīt, atspējot, nozagt aktīvu vai iegūt neatļautu piekļuvi aktīvam, vai neatļauti izmantot aktīvu un ko veic jebkurš apdraudējuma dalībnieks;

(10) “draudu izlūkdati” ir informācija, kas apkopota, pārveidota, analizēta, interpretēta vai papildināta, lai nodrošinātu vajadzīgo kontekstu lēmumu pieņemšanai un kas sniedz būtisku un pietiekamu izpratni, kā mazināt ar IKT saistīta incidenta vai kiberdraudu ietekmi, tostarp tehnisko informāciju par kiberuzbrukumu, par uzbrukumu atbildīgajām personām, to darbības veidu un motīviem;

(11) “padziļināta aizsardzība” ir ar IKT saistīta stratēģija, kas integrē cilvēkus, procesus un tehnoloģijas, lai izveidotu dažādus šķēršļus dažādos vienības slāņos un dimensijās;

(12) “neaizsargātība” ir aktīva, sistēmas, procesa vai kontroles trūkums, uzņēmība vai nepilnība, ko var izmantot draudu gadījumā;

(13) “draudu vadīta ielaušanās testēšana” ir sistēma, kura imitē tādu apdraudējuma dalībnieku taktiku, paņēmienus un procedūras, kas tiek uztverti kā patiesi kiberdraudi, un kura nodrošina kontrolētu, īpaši izstrādātu, izlūkdatu vadītu (sarkanās komandas) vienības kritiski svarīgas aktīvas izstrādes sistēmas testēšanu;

(14) “ar trešo personu saistīts IKT risks” ir IKT risks, kas finanšu vienībai var rasties saistībā ar to, ka tā izmanto trešās personas, kas sniedz IKT pakalpojumus, vai tā tālāku apakšuzņēmēju sniegtus IKT pakalpojumus;

(15) “trešā persona, kas sniedz IKT pakalpojumus” ir uzņēmums, kas sniedz digitālos un datu pakalpojumus, ieskaitot mākoņdatošanas pakalpojumu, programmatūras, datu analītikas, datu centru pakalpojumu sniedzējus, bet neskaitot aparatūras komponentu piegādātājus un uzņēmumus, kuriem saskaņā ar Savienības tiesību aktiem piešķirta atļauja un kuri sniedz elektronisko sakaru pakalpojumus, kas definēti Eiropas Parlamenta un Padomes Direktīvas (ES) 2018/1972[43] 2. panta 4. punktā;

(16) “IKT pakalpojumi” ir digitālie un datu pakalpojumi, ko ar IKT sistēmu starpniecību sniedz vienam vai vairākiem iekšējiem vai ārējiem lietotājiem, ieskaitot datu sniegšanas, datu ievadīšanas, datu glabāšanas, datu apstrādes un ziņošanas pakalpojumus, datu uzraudzības, kā arī uz datiem balstītas darījumdarbības un lēmumu pieņemšanas atbalsta pakalpojumus;

(17) “kritiski svarīga vai svarīga funkcija” ir funkcija, kuras izpildes izbeigšana, trūkumi vai neizpilde būtiski kaitētu finanšu vienības atļaujā paredzēto noteikumu un nosacījumu vai citu piemērojamajos finanšu pakalpojumu tiesību aktos paredzēto saistību turpmākai izpildei, tās finanšu rādītājiem vai tās pakalpojumu un darbību stabilitātei vai nepārtrauktībai;

(18) “kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus” ir trešā persona, kas sniedz IKT pakalpojumus, kas izraudzīta saskaņā ar 29. pantu un pakļauts 30.–37. pantā minētajai pārraudzības sistēmai;

(19) “trešā valstī reģistrēta trešā persona, kas sniedz IKT pakalpojumus” ir trešā persona, kas sniedz IKT pakalpojumus un kas ir trešā valstī reģistrēta juridiska persona, kura nav izveidojusi uzņēmumu un neatrodas Savienībā un ir noslēgusi līgumisku vienošanos ar finanšu vienību par IKT pakalpojumu sniegšanu;

[43] Eiropas Parlamenta un Padomes Direktīva (ES) 2018/1972 (2018. gada 11. decembris) par Eiropas Elektronisko sakaru kodeksa izveidi (pārstrādāta redakcija) (OV L 321, 17.12.2018., 36. lpp.).

(20) “trešā valstī reģistrēts IKT apakšuzņēmējs” ir IKT apakšuzņēmējs, kas ir trešā valstī reģistrēta juridiska persona, kura nav izveidojusi uzņēmumu un neatrodas Savienībā un ir noslēgusi līgumisku vienošanos vai nu ar trešo personu, kas sniedz IKT pakalpojumus, vai ar trešā valstī reģistrētu trešo personu, kas sniedz IKT pakalpojumus;

(21) “IKT koncentrācijas risks” ir pakļautība atsevišķām vai vairākām saistītām trešām personām, kas sniedz kritiski svarīgus IKT pakalpojumus, kas rada zināmu atkarību no šādiem pakalpojumu sniedzējiem, tā ka to nepieejamība, atteice vai cita veida trūkums var apdraudēt finanšu vienības un galu galā visas Savienības finanšu sistēmas spēju nodrošināt kritiski svarīgas funkcijas vai likt ciest cita veida nelabvēlīgas sekas, tostarp lielus zaudējumus;

(22) “vadības struktūra” ir vadības struktūra, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2014/65/ES 4. panta 1. punkta 36. apakšpunktā, Direktīvas 2013/36/ES 3. panta 1. punkta 7. apakšpunktā, Direktīvas 2009/65/EK 2. panta 1. punkta s) apakšpunktā, Regulas (ES) Nr. 909/2014 2. panta 1. punkta 45. apakšpunktā, Eiropas Parlamenta un Padomes Regulas (ES) 2016/1011[44] 3. panta 1. punkta 20. apakšpunktā, Regulas (ES) 20xx/xx[45] [KAT] 3. panta 1. punkta u) apakšpunktā, vai līdzvērtīgās personas, kuras faktiski vada vienību vai kuras pilda galvenās funkcijas saskaņā ar attiecīgajiem Savienības vai valsts tiesību aktiem;

(23) “kredītiestāde” ir kredītiestāde, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) Nr. 575/2013[46] 4. panta 1. punkta 1. apakšpunktā;

(24) “ieguldījumu brokeru sabiedrība” ir ieguldījumu brokeru sabiedrība, kā definēts Direktīvas 2014/65/ES 4. panta 1. punkta 1. apakšpunktā;

(25) “maksājumu iestāde” ir maksājumu iestāde, kā definēts Regulas (ES) 2015/2366 1. panta 1. punkta d) apakšpunktā;

(26) “elektroniskās naudas iestāde” ir elektroniskās naudas iestāde, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2009/110/EK[47] 2. panta 1. punktā;

(27) “centrālais darījumu partneris” ir centrālais darījumu partneris, kā definēts Regulas (ES) Nr. 648/2012 2. panta 1. punktā;

(28) “darījumu reģistrs” ir darījumu reģistrs, kā definēts Regulas (ES) Nr. 648/2012 2. panta 2. punktā;

(29) “centrālais vērtspapīru depozitārijs” ir centrālais vērtspapīru depozitārijs, kā definēts Regulas (ES) Nr. 909/2014 2. panta 1. punkta 1. apakšpunktā;

---

44 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.).

45 [*Lūdzu, ievietojiet pilnu nosaukumu un OV informāciju*].

46 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.).

47 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.).

(30) “tirdzniecības vieta” ir tirdzniecības vieta, kā definēts Direktīvas 2014/65/ES 4. panta 1. punkta 24. apakšpunktā;

(31) “alternatīvo ieguldījumu fondu pārvaldnieks” ir alternatīvo ieguldījumu fondu pārvaldnieks, kā definēts Direktīvas 2011/61/EK 4. panta 1. punkta b) apakšpunktā;

(32) “pārvaldības sabiedrība” ir pārvaldības sabiedrība, kā definēts Direktīvas 2009/65/EK 2. panta 1. punkta b) apakšpunktā;

(33) “datu ziņošanas pakalpojumu sniedzējs” ir datu ziņošanas pakalpojumu sniedzējs, kā definēts Direktīvas 2014/65/ES 4. panta 1. punkta 63. apakšpunktā;

(34) “apdrošināšanas sabiedrība” ir apdrošināšanas sabiedrība, kā definēts Direktīvas 2009/138/EK 13. panta 1. punktā;

(35) “pārapdrošināšanas sabiedrība” ir pārapdrošināšanas sabiedrība, kā definēts Direktīvas 2009/138/EK 13. panta 4. punktā;

(36) “apdrošināšanas starpnieks” ir apdrošināšanas starpnieks, kā definēts Direktīvas (ES) 2016/97 2. panta 3. punktā;

(37) “apdrošināšanas papildpakalpojuma starpnieks” ir apdrošināšanas papildpakalpojuma starpnieks, kā definēts Direktīvas (ES) 2016/97 2. panta 4. punktā;

(38) “pārapdrošināšanas starpnieks” ir pārapdrošināšanas starpnieks, kā definēts Direktīvas (ES) 2016/97 2. panta 5. punktā;

(39) “arodpensijas kapitāla uzkrāšanas institūcija” ir arodpensijas kapitāla uzkrāšanas institūcija, kā definēts Direktīvas 2016/2341 6. panta 1. punktā;

(40) “kredītreitingu aģentūra” ir kredītreitingu aģentūra, kā definēts Regulas (EK) Nr. 1060/2009 3. panta 1. punkta b) apakšpunktā;

(41) “obligātais revidents” ir obligātais revidents, kā definēts Direktīvas 2006/43/EK 2. panta 2. punktā;

(42) “revīzijas uzņēmums” ir revīzijas uzņēmums, kā definēts Direktīvas 2006/43/EK 2. panta 3. punktā;

(43) “kriptoaktīvu pakalpojumu sniedzējs” ir kriptoaktīvu pakalpojumu sniedzējs, kā definēts Regulas (ES) 202x/xx 3. panta 1. punkta n) apakšpunktā [*PB*: *ievietot atsauci uz KAT regulu*];

(44) “kriptoaktīvu emitents” ir kriptoaktīvu emitents, kā definēts 3. panta 1. punkta h) apakšpunktā [*OV: ievietot atsauci uz KAT regulu*];

(45) “aktīviem piesaistītu tokenu emitents” ir aktīviem piesaistītu tokenu emitents, kā definēts [*OV*: *ievietot atsauci uz KAT regulu*] 3. panta 1. punkta i) apakšpunktā;

(46) “nozīmīgu aktīviem piesaistītu tokenu emitents” ir nozīmīgu aktīviem piesaistītu tokenu emitents, kā definēts [*OV*: *ievietot atsauci uz KAT regulu*] 3. panta 1. punkta j) apakšpunktā;

(47) “kritiski svarīgu etalonu administrators” ir kritiski svarīgu etalonu administrators, kā definēts Regulas xx/202x [*OV*: *ievietot atsauci uz Etalonu regulu*] x. panta x. punktā;

(48) “kolektīvās finansēšanas pakalpojumu sniedzējs” ir kolektīvās finansēšanas pakalpojumu sniedzējs, kā definēts Regulas (ES) 202x/xx [*PB*: *ievietot atsauci uz Kolektīvās finansēšanas regulu*] x. panta x. punktā;

(49) “vērtspapīrošanas repozitorijs” ir vērtspapīrošanas repozitorijs, kā definēts Regulas (ES) 2017/2402 2. panta 23. punktā;

(50) “mikrouzņēmums” ir finanšu vienība, kā definēts Ieteikuma 2003/361/EK pielikuma 2. panta 3. punktā.

II NODAĻA

IKT RISKA PĀRVALDĪBA

I IEDAĻA

4. pants

Pārvaldība un organizācija

1. Finanšu vienībām ir izveidotas iekšējās pārvaldības un kontroles sistēmas, kas nodrošina visu IKT risku efektīvu un prudenciālu pārvaldību.

2. Finanšu vienības vadības struktūra nosaka, apstiprina, pārrauga un atbild par visu ar 5. panta 1. punktā minēto IKT riska pārvaldības sistēmu saistīto pasākumu īstenošanu:

Pirmās daļas īstenošanas vajadzībām vadības struktūra:

(a) galīgi atbild par finanšu vienības IKT risku pārvaldību;

(b) nosaka visu ar IKT saistīto funkciju uzdevumus un atbildību;

(c) nosaka atbilstīgu finanšu vienības IKT riska tolerances līmeni, kā minēts 5. panta 9. punkta b) apakšpunktā;

(d) apstiprina, pārrauga un periodiski pārskata attiecīgi 10. panta 1. un 3. punktā minētās finanšu vienības IKT darbības nepārtrauktības politikas un IKT negadījuma seku novēršanas plāna īstenošanu;

(e) apstiprina un periodiski pārskata IKT revīzijas plānus, IKT revīzijas un būtiskus to grozījumus;

(f) piešķir un periodiski pārskata atbilstīgu budžetu, lai apmierinātu finanšu vienības digitālās darbības noturības vajadzības attiecībā uz visu veidu resursiem, ieskaitot visu attiecīgo darbinieku apmācību par IKT riskiem un prasmēm;

(g) apstiprina un periodiski pārskata finanšu vienības rīcībpolitiku attiecībā uz kārtību, kādā tiek izmantoti IKT pakalpojumi, ko sniedz IKT pakalpojumus sniedzošās trešās personas;

(h) tiek pienācīgi informēta par nolīgumiem, kas ir noslēgti ar IKT pakalpojumus sniedzošajām trešām personām par IKT pakalpojumu izmantošanu, attiecīgām plānotām būtiskām izmaiņām attiecībā uz trešām personām, kas sniedz IKT pakalpojumus, un šo izmaiņu iespējamo ietekmi uz kritiski svarīgām vai svarīgām funkcijām, kam piemēro nolīgumus, tajā skaitā saņem riska analīzes kopsavilkumu, lai izvērtētu šo izmaiņu ietekmi;

(i) tiek pienācīgi informēta par incidentiem, kas saistīti ar IKT, un to ietekmi, kā arī reaģēšanas, seku novēršanas un korektīvajiem pasākumiem.

3. Finanšu vienības, kas nav mikrouzņēmumi, izveido funkciju, ar kuru uzrauga ar trešām personām, kas sniedz IKT pakalpojumus, noslēgtos nolīgumus par IKT pakalpojumu izmantošanu, vai ieceļ augstākās vadības locekli, kas atbild par to, lai tiktu uzraudzīta pakļautība riskam un attiecīgie dokumenti.

4. Vadības struktūras locekļi regulāri iziet īpašu mācību kursu, lai iegūtu un atjauninātu pietiekamas zināšanas un prasmes, kas ļauj saprast un novērtēt IKT riskus un to ietekmi uz finanšu vienības darbību.

II IEDAĻA

5. pants

IKT riska pārvaldības sistēma

1. Finanšu vienībām ir stabila, visaptveroša un labi dokumentēta IKT riska pārvaldības sistēma, kas tām ļauj ātri, efektīvi un visaptveroši novērst IKT riskus un nodrošināt augstu digitālās darbības noturības līmeni, kas atbilst to darījumdarbības vajadzībām, lielumam un sarežģītībai.

2. Šā panta 1. punktā minētā IKT riska pārvaldības sistēma ietver stratēģijas, rīcībpolitiku, procedūras, IKT protokolus un rīkus, kas vajadzīgi, lai pienācīgi un efektīvi aizsargātu visas attiecīgās fiziskās sastāvdaļas un infrastruktūras, tostarp datortehniku, serverus, kā arī visas attiecīgās telpas, datu centrus un par sensitīvām noteiktās teritorijas, lai nodrošinātu, ka visi šie fiziskie elementi ir pienācīgi aizsargāti no riskiem, tostarp bojājumiem un neatļautas piekļuves vai izmantošanas.

3. Finanšu vienības mazina IKT risku ietekmi, ieviešot IKT riska pārvaldības sistēmā noteiktās attiecīgās stratēģijas, rīcībpolitiku, procedūras, protokolus un rīkus. Tās sniedz kompetento iestāžu noteikto pilnīgo un aktualizēto informāciju par IKT riskiem.

4. Finanšu vienības, kas nav mikrouzņēmumi, kā daļu no 1. punktā minētās IKT riska pārvaldības sistēmas īsteno uz atzītiem starptautiskiem standartiem balstītu informācijas drošības pārvaldības sistēmu, ievērojot uzraudzības norādījumus, un regulāri to pārskata.

5. Finanšu vienības, kas nav mikrouzņēmumi, nodrošina IKT vadības funkciju, kontroles funkciju un iekšējās revīzijas funkciju pienācīgu nošķiršanu atbilstīgi trīs aizsardzības līniju modelim vai iekšējam riska pārvaldības un kontroles modelim.

6. Šā panta 1. punktā minēto IKT riska pārvaldības sistēmu dokumentē un pārskata vismaz reizi gadā, kā arī pēc būtisku ar IKT saistītu incidentu iestāšanās, ievērojot uzraudzības norādījumus vai attiecīgos digitālās darbības noturības testēšanas un revīzijas procesos gūtos secinājumus. To pastāvīgi uzlabo, balstoties uz īstenošanas un uzraudzības gaitā gūtajām atziņām.

7. IKT revidenti, kam ir pietiekamas zināšanas, prasmes un zinātība par IKT risku, regulāri veic 1. punktā minētās IKT riska pārvaldības sistēmas revīziju. IKT revīzijas biežums un tajā galvenokārt pievērstā uzmanība ir samērīga ar finanšu vienības IKT riskiem.

8. Izveido oficiālu turpmākās pārraudzības procesu, tostarp noteikumus par kritiski svarīgu IKT revīzijas konstatējumu laicīgu pārbaudi un izlabošanu, ņemot vērā revīzijas pārskata secinājumus un vienlaikus pienācīgi apsverot finanšu vienības pakalpojumu un darbības būtību, apjomu un sarežģītību.

9. Šā panta 1. punktā minētā IKT riska pārvaldības sistēma ietver digitālās darbības noturības stratēģiju, kurā izklāstīts, kā sistēma tiek īstenota. Šajā nolūkā tā ietver metodes, kā novērst IKT risku un sasniegt konkrētus IKT mērķus:

(a) izskaidrojot, kā IKT riska pārvaldības sistēma atbalsta finanšu vienības darījumdarbības stratēģiju un mērķus;

(b) nosakot riska tolerances līmeni IKT riskam saskaņā ar finanšu vienības gatavību uzņemties risku, kā arī analizējot IKT traucējumu ietekmes noturību;

(c) nosakot skaidrus informācijas drošības mērķus;

(d) izskaidrojot IKT atsauces arhitektūru un jebkādas izmaiņas, kas vajadzīgas, lai sasniegtu konkrētus darījumdarbības mērķus;

(e) izklāstot dažādos mehānismus, kas ieviesti, lai atklātu, aizsargātu un novērstu ar IKT saistītu incidentu ietekmi;

(f) pamatojot paziņoto būtisko ar IKT saistīto incidentu skaitu un preventīvo pasākumu efektivitāti;

(g) vienības līmenī nosakot visaptverošu IKT vairāku piegādātāju stratēģiju, norādot svarīgākās atkarības no trešām personām, kas sniedz IKT pakalpojumus, un izskaidrojot trešo personu, kas sniedz pakalpojumus, iepirkuma loka pamatojumu;

(h) īstenojot digitālās darbības noturības testēšanu;

(i) izklāstot saziņas stratēģiju ar IKT saistīta incidenta gadījumā.

10. Pēc kompetento iestāžu apstiprinājuma finanšu vienības var deleģēt IKT riska pārvaldības prasību izpildes pārbaudes uzdevumus grupas iekšienē vai ārējiem uzņēmumiem.

6. pants

IKT sistēmas, protokoli un rīki

1. Finanšu vienības izmanto un uztur aktualizētas IKT sistēmas, protokolus un rīkus, kas atbilst šādiem nosacījumiem:

(a) sistēmas un rīki ir piemēroti operāciju būtībai, daudzveidībai, sarežģītībai un apjomam, ar ko tiek atbalstīta to darbība;

(b) tie ir uzticami;

(c) tiem ir pietiekama veiktspēja, lai precīzi apstrādātu laicīgai darbību veikšanai un pakalpojumu sniegšanai nepieciešamos datus, kā arī pēc vajadzības apstrādātu rīkojumu, ziņojumu vai darījumu maksimālos apjomus, tajā skaitā — ja tiek ieviesta jauna tehnoloģija;

(d) tie ir tehnoloģiski elastīgi, lai pienācīgi risinātu papildu informācijas apstrādes vajadzības, kas nepieciešams saspringtos tirgus apstākļos vai citās nelabvēlīgās situācijās.

2. Ja finanšu vienības izmanto starptautiski atzītus tehniskos standartus un nozares paraugpraksi informācijas drošības un IKT iekšējās kontroles jomā, tās šos standartus un praksi izmanto atbilstīgi attiecīgiem uzraudzības norādījumiem par to iekļaušanu.

7. pants

Identifikācija

1. Regulas 5. panta 1. punktā minētās IKT riska pārvaldības sistēmas ietvaros finanšu vienības identificē, klasificē un pienācīgi dokumentē visas ar IKT saistītās darījumdarbības funkcijas, šo funkciju atbalsta informācijas aktīvus, kā arī IKT sistēmas konfigurācijas un savstarpējos savienojumus ar iekšējām un ārējām IKT sistēmām. Finanšu vienības pēc vajadzības, bet ne retāk kā reizi gadā izvērtē informācijas aktīvu un attiecīgu dokumentu klasifikācijas piemērotību.

2. Finanšu vienības pastāvīgi identificē visus IKT riska avotus, jo īpaši pakļautību riskam, kur iesaistītas citas finanšu vienības, un izvērtē kiberdraudus un IKT neaizsargātību, kam ir nozīme to ar IKT saistītajās darījumdarbības funkcijās un informācijas aktīvos. Finanšu vienības regulāri, bet ne retāk kā reizi gadā izvērtē riska scenārijus, kas tās ietekmē.

3. Finanšu vienības, kas nav mikrouzņēmumi, pēc katrām būtiskām tīklu un informācijas sistēmas infrastruktūras, procesu vai procedūru izmaiņām, kas ietekmē to darbību, atbalsta procesus vai informācijas aktīvus, veic riska novērtējumu.

4. Finanšu vienības identificē visus IKT sistēmas kontus, tostarp tos, kas atrodas attālās vietnēs, tīkla resursus un aparatūras iekārtas, un kartē par kritiski svarīgām uzskatītas fiziskas iekārtas. Tās kartē IKT aktīvu konfigurāciju, kā arī dažādu IKT aktīvu saites un savstarpējo atkarību.

5. Finanšu vienības identificē un dokumentē visus procesus, kas ir atkarīgi no trešām personām, kas sniedz IKT pakalpojumus, un identificē savstarpējus savienojumus ar trešām personām, kas sniedz IKT pakalpojumus.

6. Šā panta 1., 4. un 5. punkta nolūkiem finanšu vienības uztur un regulāri aktualizē attiecīgos inventāra sarakstus.

7. Finanšu vienības, kas nav mikrouzņēmumi, regulāri un vismaz reizi gadā veic visu mantoto IKT sistēmu IKT riska īpašu novērtējumu, jo sevišķi pirms veco un jauno tehnoloģiju, lietojumprogrammu vai sistēmu savienošanas, kā arī pēc tās.

8. pants

Aizsardzība un profilakse

1. Lai pienācīgi aizsargātu IKT sistēmas un ar mērķi organizēt reaģēšanas pasākumus, finanšu vienības pastāvīgi uzrauga un kontrolē IKT sistēmu un rīku darbību, kā arī mazina šādu risku ietekmi, ieviešot attiecīgus IKT drošības rīkus, rīcībpolitiku un procedūras.

2. Finanšu vienības izstrādā, sagādā un īsteno IKT drošības stratēģijas, rīcībpolitiku, procedūras, protokolus un rīkus, kuru mērķis ir jo īpaši nodrošināt IKT sistēmu noturību, nepārtrauktību un pieejamību, kā arī uzturēt augstus datu drošības, konfidencialitātes un integritātes standartus neatkarīgi no tā, vai tie tiek glabāti, lietoti vai pārsūtīti.

3. Lai sasniegtu 2. punktā minētos mērķus, finanšu vienības izmanto mūsdienīgas IKT tehnoloģijas un procesus, kas:

   (a) garantē informācijas pārsūtīšanas līdzekļu drošību;

(b) mazina datu bojājumu vai zudumu, neatļautas piekļuves un tehnisko nepilnību, kas varētu kavēt darījumdarbību, risku;

(c) novērš informācijas noplūdi;

(d) nodrošina datu aizsardzību pret sliktas pārvaldības vai apstrādes riskiem, ieskaitot nepilnīgu uzskaiti.

4. Šā panta 5. panta 1. punktā minētās IKT riska pārvaldības sistēmas ietvaros finanšu vienības:

(a) izstrādā un dokumentē informācijas drošības politiku, paredzot noteikumus savu un klientu IKT resursu, datu un informācijas aktīvu konfidencialitātes, integritātes un pieejamības aizsardzībai;

(b) izmantojot uz risku balstītu pieeju, izveido stabilu tīkla un infrastruktūras pārvaldību, lietojot attiecīgus paņēmienus, metodes un protokolus, tajā skaitā ieviešot automatizētus mehānismus, ar kuriem izolēt skartos informācijas aktīvus kiberuzbrukuma gadījumā;

(c) īsteno rīcībpolitiku, kas ierobežo fizisku un virtuālu piekļuvi IKT sistēmas resursiem un datiem tādā apjomā, kāds ir nepieciešams leģitīmām un atļautām funkcijām un darbībām, un šim nolūkam izveido rīcībpolitikas, procedūru un kontroles pasākumu kopumu, kurā ir noteiktas piekļuves tiesības un to pareiza pārvaldība;

(d) īsteno rīcībpolitiku un protokolus, kas paredz spēcīgus autentificēšanas mehānismus, kuri ir balstīti uz attiecīgiem standartiem un īpašām kontroles sistēmām, kas liedz piekļūt šifrēšanas atslēgām, ar kurām tiek šifrēti dati, balstoties uz apstiprinātiem datu klasifikācijas un riska novērtējuma procesiem;

(e) īsteno IKT izmaiņu, tostarp programmatūras, aparatūras, aparātprogrammatūras komponentu, sistēmas vai drošības izmaiņu, pārvaldības politiku, procedūras un kontroles, kas ir balstītas uz riska pārvaldības pieeju un ir finanšu vienības kopējās izmaiņu pārvaldības politikas neatņemama daļa, lai nodrošinātu, ka visas IKT sistēmu izmaiņas tiek kontrolēti reģistrētas, testētas, novērtētas, apstiprinātas, ieviestas un pārbaudītas;

(f) ievieš attiecīgu un visaptverošu labojumu un atjauninājumu politiku.

Šā punkta b) apakšpunkta mērķiem finanšu vienības projektē tīkla savienojuma infrastruktūru tā, lai to varētu nekavējoties pārtraukt tās darbību, un nodrošina tās nodalījumu veidošanu un segmentāciju, lai mazinātu kaitīgas ietekmes izplatīšanos, jo īpaši attiecībā uz savstarpēji savienotiem finanšu procesiem.

Šā punkta e) apakšpunkta vajadzībām IKT izmaiņu pārvaldības procesu apstiprina atbilstīga hierarhiskā vadība, un tam ir īpaši protokoli, kas ļauj veikt ārkārtas izmaiņas.

9. pants

Atklāšana

1. Finanšu vienības saskaņā ar 15. pantu ievieš mehānismus, lai nekavējoties atklātu anomālas darbības, ieskaitot IKT tīkla veiktspējas problēmas un ar IKT saistītus incidentus, kā arī identificētu visas iespējamās būtiskās atsevišķu ķēdes punktu kļūdainas darbības.

Visus pirmajā daļā minētos atklāšanas mehānismus regulāri testē saskaņā ar 22. pantu.

2. Šā panta 1. punktā minētie atklāšanas mehānismi ļauj veikt vairākslāņu kontroli, nosaka brīdināšanas mehānismu robežvērtības un kritērijus, atbilstīgi kuriem tiek ierosināti ar IKT saistīto incidentu atklāšanas un ar IKT saistīto incidentu reaģēšanas procesi, kā arī ievieš automātiskus mehānismus, lai brīdinātu attiecīgo personālu, kas atbild par reaģēšanu uz incidentiem, kas saistīti ar IKT.

3. Finanšu vienības, pienācīgi ņemot vērā to lielumu, darījumdarbības un riska profilus, atvēl pietiekamus resursus un spējas, ar ko uzraudzīt lietotāju darbības, IKT anomāliju un ar IKT saistīto incidentu, jo īpaši kiberuzbrukumu, iestāšanos.

4. Regulas 2. panta 1. punkta 1. apakšpunktā minētās finanšu vienības papildus minētajam ir ieviesušas sistēmas, kas ļauj efektīvi pārbaudīt tirdzniecības ziņojumu pilnīgumu, identificēt izlaidumus un acīm redzamas kļūdas, kā arī pieprasīt kļūdainu ziņojumu atkārtotu nosūtīšanu.

10. pants

Reaģēšana un seku novēršana

1. Regulas 5. panta 1. punktā minētās IKT riska pārvaldības sistēmas ietvaros un pamatojoties uz 7. pantā noteiktajām identifikācijas prasībām, finanšu vienības ievieš īpašu un visaptverošu IKT darbības nepārtrauktības politiku kā finanšu vienības darbības nepārtrauktības politikas neatņemamu daļu.

2. Finanšu vienības īsteno 1. punktā minēto IKT darbības nepārtrauktības politiku, izmantojot īpašu, piemērotu un dokumentētu kārtību, plānus, procedūras un mehānismus, kuru mērķis ir:

   (a) reģistrēt visus ar IKT saistītos incidentus;

   (b) nodrošināt finanšu vienības kritiski svarīgo funkciju nepārtrauktību;

   (c) ātri, pienācīgi un efektīvi reaģēt uz visiem ar IKT saistītajiem incidentiem un novērst tos, cita starpā jo īpaši kiberuzbrukumus, tā, lai ierobežotu kaitējumu un par prioritārām noteiktu darbības atsākšanu un seku novēršanu;

   (d) nekavējoties aktivizēt īpašus plānus, kas ļauj īstenot ierobežošanas pasākumus, procesus un tehnoloģijas, kuri piemēroti katram ar IKT saistītajam incidentam un ļauj novērst turpmāku kaitējumu, kā arī pielāgotas reaģēšanas un atgūšanas procedūras, kas noteiktas saskaņā ar 11. pantu;

   (e) provizoriski aplēst ietekmi, kaitējumu un zaudējumus;

   (f) noteikt saziņas un krīzes pārvarēšanas pasākumus, kas nodrošina atjauninātas informācijas nosūtīšanu visiem attiecīgajiem iekšējiem darbiniekiem un ārējām ieinteresētajām personām saskaņā ar 13. pantu un tās paziņošanu kompetentajām iestādēm saskaņā ar 17. pantu.

3. Regulas 5. panta 1. punktā minētās IKT riska pārvaldības sistēmas ietvaros finanšu vienības īsteno saistītu IKT negadījuma seku novēršanas plānu, kuram finanšu vienības, kas nav mikrouzņēmumi, veic neatkarīgu revīzijas pārskatīšanu.

4. Finanšu vienības ievieš, uztur un periodiski testē attiecīgus IKT darbības nepārtrauktības plānus, jo īpaši attiecībā uz kritiski svarīgām vai svarīgām funkcijām,

kas ir uzticētas ārpakalpojumā vai par ko noslēgts līgums ar trešām personām, kas sniedz IKT pakalpojumus.

5. Finanšu vienības kā daļu no visaptverošās IKT riska pārvaldības:

(a) vismaz reizi gadā un pēc būtiskām IKT sistēmu izmaiņām testē IKT darbības nepārtrauktības politiku un IKT negadījuma seku novēršanas plānu;

(b) testē saskaņā ar 13. pantu izveidotos krīzes saziņas plānus.

Šā punkta a) apakšpunkta vajadzībām finanšu vienības, kas nav mikrouzņēmumi, testēšanas plānos iekļauj scenārijus, kuros notiek kiberuzbrukumi un pārslēgšanās starp primāro IKT infrastruktūru un rezerves jaudu, rezerves kopijām un rezerves mehānismiem, kas vajadzīgi 11. pantā noteikto pienākumu izpildei.

Finanšu vienības regulāri pārskata savu IKT darbības nepārtrauktības politiku un IKT negadījuma seku novēršanas plānu, ņemot vērā saskaņā ar panta pirmo daļu veikto testu rezultātus un ieteikumus, kas izriet no revīzijas pārbaudēm vai uzraudzības pārskatiem.

6. Finanšu vienībām, kas nav mikrouzņēmumi, ir krīzes pārvarēšanas funkcija, kurā IKT darbības nepārtrauktības politikas vai IKT negadījuma seku novēršanas plāna aktivizēšanas gadījumā ir jāparedz skaidras procedūras, kā pārvaldīt iekšējo un ārējo krīzes saziņu saskaņā ar 13. pantu.

7. Finanšu vienības uztur reģistru, kurā ietver pirms traucējuma un traucējuma laikā veiktās darbības, ja tikusi aktivizēta IKT darbības nepārtrauktības politika vai IKT negadījuma seku novēršanas plāns. Tā ieraksti ir viegli pieejami.

8. Regulas 2. panta 1. punkta f) apakšpunktā minētās finanšu vienības iesniedz kompetentajām iestādēm pārskata periodā veikto IKT darbības nepārtrauktības testu vai līdzīgu izmēģinājumu rezultātu kopijas.

9. Finanšu vienības, kas nav mikrouzņēmumi, ziņo kompetentajām iestādēm par visām izmaksām un zaudējumiem, ko izraisījuši IKT traucējumi un ar IKT saistītie incidenti.

11. pants

Rezerves kopiju veidošanas politika un atgūšanas metodes

1. Lai nodrošinātu IKT sistēmu atkopšanu ar minimāliem laika zaudējumiem un ierobežotiem traucējumiem, finanšu vienības kā daļu no IKT riska pārvaldības sistēmas izstrādā:

(a) rezerves kopiju veidošanas politiku, kurā nosaka datus, kuriem veido rezerves kopijas, un rezerves kopiju veidošanas minimālo biežumu, balstoties uz informācijas svarīgumu vai datu sensitivitāti;

(b) atgūšanas metodes.

2. Rezerves sistēmas apstrādi sāk bez nepamatotas kavēšanās, izņemot, ja šī uzsākšana apdraudētu tīklu un informācijas sistēmu drošību vai datu integritāti vai konfidencialitāti.

3. Kad, izmantojot savas sistēmas, tiek atjaunoti rezerves kopijas dati, finanšu vienības izmanto IKT sistēmas, kuru darbības vide ir atšķirīga no galvenās, kuras nav tieši savienotas ar to un kuras ir droši aizsargātas no neatļautas piekļuves vai IKT bojājumiem.

Regulas 2. panta 1. punkta g) apakšpunktā minēto finanšu vienību atgūšanas plāni atļauj atjaunot visus darījumus kopš pārtraukšanas brīža, lai centrālais darījumu partneris varētu turpināt droši darboties un pabeigt norēķinus paredzētajā dienā.

4. Finanšu vienības uztur rezerves IKT jaudu, kam ir darījumdarbības vajadzību nodrošināšanai pietiekami un piemēroti resursi, spējas un funkcionalitāte.

5. Regulas 2. panta 1. punkta f) apakšpunktā minētās finanšu vienības nodrošina vai panāk, ka to trešās personas, kas sniedz IKT pakalpojumus, uztur vismaz vienu rezerves apstrādes vietu, kam ir darījumdarbības vajadzību nodrošināšanai piemēroti un pietiekami resursi, spējas, funkcionalitāte un personāls.

Rezerves apstrādes vieta:

(a) atrodas ģeogrāfiski attālu no galvenās apstrādes vietas, lai nodrošinātu, ka tai ir atšķirīgs riska profils, un novērstu, ka to skar notikums, kas ir skāris galveno vietu;

(b) spēj nodrošināt kritiski svarīgu pakalpojumu nepārtrauktību tieši tāpat kā galvenā vieta vai sniegt pakalpojumus līmenī, kas nepieciešams, lai nodrošinātu, ka finanšu vienība veic kritiski svarīgās darbības saskaņā ar atgūšanas mērķiem;

(c) ir nekavējoties pieejama finanšu vienības personālam, lai nodrošinātu kritiski svarīgu pakalpojumu nepārtrauktību, ja galvenā apstrādes vieta ir kļuvusi nepieejama.

6. Nosakot katras funkcijas atgūšanas laiku un punkta mērķus, finanšu vienības ņem vērā iespējamo kopējo ietekmi uz tirgus efektivitāti. Šie laika mērķi nodrošina noteiktā pakalpojumu līmeņa izpildi ekstremālos scenārijos.

7. Novēršot ar IKT saistītā incidenta sekas, finanšu vienības veic vairākas pārbaudes, ieskaitot saskaņošanu, lai nodrošinātu, ka datu integritāte ir visaugstākajā līmenī. Šīs pārbaudes veic arī, atjaunojot datus no ārējām ieinteresētajām personām, lai nodrošinātu, ka sistēmu dati ir savstarpēji sakritīgi.

12. pants

Mācīšanās un attīstība

1. Finanšu vienībām ir to lielumam, darījumdarbības un riska profiliem pieskaņotas spējas un personāls, lai apkopotu informāciju par neaizsargātību un kiberdraudiem, ar IKT saistītiem incidentiem, jo īpaši kiberuzbrukumiem, un analizētu to iespējamo ietekmi uz to digitālās darbības noturību.

2. Finanšu vienības ievieš ar IKT saistītu incidentu pārskatīšanu pēc būtiskiem IKT traucējumiem to pamatdarbībā, analizējot traucējumu cēloņus un nosakot nepieciešamos uzlabojumus IKT darbībās vai IKT darbības nepārtrauktības politikā, kas minēta 10. pantā.

Ieviešot izmaiņas, finanšu vienības, kas nav mikrouzņēmumi, par šīm izmaiņām paziņo kompetentajām iestādēm.

Pirmajā daļā minētajā ar IKT saistītā incidenta pārskatīšanā nosaka, vai tika ievērotas noteiktās procedūras un vai veiktās darbības bija efektīvas, tostarp attiecībā uz:

(a) tūlītēju reaģēšanu uz drošības brīdinājumiem un ar IKT saistīto incidentu ietekmes un to būtiskuma noteikšanu;

(b) kriminālistikas analīzes kvalitāti un ātrumu;

(c) incidentu eskalācijas efektivitāti finanšu vienībā;

(d) iekšējās un ārējās saziņas efektivitāti.

3. IKT riska novērtējuma procesā pastāvīgi iekļauj pieredzi, kas gūta saskaņā ar 23. un 24. pantu veiktās digitālās darbības noturības testos un no reāliem ar IKT saistītiem incidentiem, jo īpaši kiberuzbrukumiem, kā arī saistībā ar problēmām, ar ko saskaras, aktivizējot darbības nepārtrauktības vai seku novēršanas plānus, kopā ar attiecīgo informāciju, kas koplietota ar darījumu partneriem un novērtēta uzraudzības pārbaudēs. Šie konstatējumi attiecīgi ļauj pārskatīt 5. panta 1. punktā minētās IKT riska pārvaldības sistēmas būtiskās sastāvdaļas.

4. Finanšu vienības uzrauga 5. panta 9. punktā noteiktās digitālās darbības noturības stratēģijas īstenošanas efektivitāti. Tās kartē IKT risku attīstību laika gaitā, analizē ar IKT saistīto incidentu biežumu, veidus, mērogu un attīstību, jo īpaši kiberuzbrukumus un to modeļus, lai izprastu, cik lielā mērā tās ir pakļautas IKT riskam, un palielinātu finanšu vienības kiberbriedumu un sagatavotību.

5. Augstākā līmeņa IKT darbinieki vismaz reizi gadā ziņo vadības struktūrai par 3. punktā minētajiem konstatējumiem un sniedz ieteikumus.

6. Finanšu vienības savās personāla apmācības shēmās kā obligātos moduļus izstrādā IKT drošības izpratnes veidošanas programmas un digitālās darbības noturības mācības. Tās attiecas uz visiem darbiniekiem un augstākās vadības personālu.

Finanšu vienības pastāvīgi uzrauga attiecīgo tehnoloģisko attīstību, lai izprastu šādu jaunu tehnoloģiju ieviešanas iespējamo ietekmi uz IKT drošības prasībām un digitālās darbības noturību. Tās seko jaunākajiem IKT riska pārvaldības procesiem, efektīvi pretojoties pašreizējām vai jaunām kiberuzbrukumu formām.

13. pants

Saziņa

1. Regulas 5. panta 1. punktā minētās IKT riska pārvaldības sistēmas ietvaros finanšu vienībām ir saziņas plāni, kas ļauj ar IKT saistītos incidentus vai lielu neaizsargātību nepieciešamības gadījumā atbildīgi atklāt klientiem un darījumu partneriem, kā arī sabiedrībai.

2. Regulas 5. panta 1. punktā minētās IKT riska pārvaldības sistēmas ietvaros finanšu vienības īsteno saziņas politiku attiecībā uz personālu un ārējām ieinteresētajām personām. Personāla apzināšanas politikā ņem vērā vajadzību nošķirt personālu, kas ir jāinformē, no IKT riska pārvaldībā, jo īpaši reaģēšanā un seku novēršanā, iesaistītā personāla.

3. Vismaz vienai personai vienībā ir uzdots īstenot saziņas stratēģiju ar IKT saistītu incidentu gadījumā un šim nolūkam pildīt runaspersonas lomu saziņā ar sabiedrību un plašsaziņas līdzekļiem.

14. pants

IKT riska pārvaldības rīku, metožu, procesu un politikas tālāka saskaņošana

Eiropas banku iestāde (EBI), Eiropas Vērtspapīru un tirgu iestāde (EVTI) un Eiropas Apdrošināšanas un aroda pensiju iestāde (EAAPI), apspriežoties ar Eiropas Savienības

Kiberdrošības aģentūru (*ENISA*), izstrādā regulatīvo tehnisko standartu projektus šādiem mērķiem:

(a) noteikt papildu elementus, kas jāiekļauj 8. panta 2. punktā minētajā IKT drošības rīcībpolitikā, procedūrās, protokolos un rīkos, lai nodrošinātu tīklu drošību, ļautu īstenot atbilstošus aizsardzības pasākumus pret ielaušanos un datu ļaunprātīgu izmantošanu, saglabātu datu autentiskumu un integritāti, tostarp kriptogrāfijas metodes, un garantētu datu precīzu un ātru pārraidi bez būtiskiem traucējumiem;

(b) noteikt, kā 8. panta 2. punktā minētā IKT drošības rīcībpolitika, procedūras un rīki ietver sistēmās drošības kontroli jau sākotnēji (integrēto drošību), ļauj pielāgoties mainīgajai apdraudējuma videi un paredz, ka tiek izmantotas padziļinātas aizsardzības tehnoloģijas;

(c) sīkāk noteikt 8. panta 4. punkta b) apakšpunktā minētos attiecīgos paņēmienus, metodes un protokolus;

(d) izstrādāt papildu komponentus 8. panta 4. punkta c) apakšpunktā minētajai piekļuves pārvaldības tiesību kontrolei un ar to saistīto cilvēkresursu politiku, lai precizētu piekļuves tiesības, tiesību piešķiršanas un anulēšanas procedūras, uzraudzītu anomālu rīcību saistībā ar IKT riskiem, izmantojot atbilstošus rādītājus, tostarp tīkla izmantošanas modeļus, laikus, IT darbību un nezināmas ierīces;

(e) sīkāk izstrādāt 9. panta 1. punktā noteiktos elementus, kas ļautu operatīvi atklāt anomālas darbības, un 9. panta 2. punktā minētos kritērijus, kas ierosina ar IKT saistītu incidentu atklāšanas un reaģēšanas procesus;

(f) sīkāk noteikt 10. panta 1. punktā minētās IKT darbības nepārtrauktības politikas komponentus;

(g) sīkāk noteikt 10. panta 5. punktā minēto IKT darbības nepārtrauktības plānu testēšanu, lai nodrošinātu, ka tajos pienācīgi ņemti vērā scenāriji, kuros kritiski svarīgas vai svarīgas funkcijas nodrošināšanas kvalitāte nepieņemami pasliktinās vai netiek ievērota vispār, un pienācīgi apsvērta attiecīgās trešās personas, kas sniedz IKT pakalpojumus, maksātnespējas vai citas atteices iespējamā ietekme un konkrētā gadījumā — attiecīgo pakalpojumu sniedzēju jurisdikciju politiskie riski;

(h) sīkāk noteikt 10. panta 3. punktā minētā IKT negadījuma seku novēršanas plāna komponentus;

EUI iesniedz Komisijai minēto regulatīvo tehnisko standartu projektus līdz [*OV: ievietot datumu, kas ir vienu gadu pēc spēkā stāšanās dienas*].

Komisijai tiek deleģētas pilnvaras pieņemt šā panta pirmajā daļā minētos regulatīvos tehniskos standartus attiecīgi saskaņā ar 10.–14. pantu Regulā (ES) Nr. 1093/2010, Regulā (ES) Nr. 1094/2010 un Regulā (ES) Nr. 1095/2010.

III NODAĻA

AR IKT SAISTĪTI INCIDENTI

PĀRVALDĪBA, KLASIFIKĀCIJA un ZIŅOŠANA

15. pants

Ar IKT saistītu incidentu pārvaldības process

1. Finanšu vienības izveido un īsteno ar IKT saistītu incidentu pārvaldības procesu, lai atklātu ar IKT saistītus incidentus, pārvaldītu tos un ziņotu par tiem, un ievieš agrīnās brīdināšanas rādītājus kā brīdinājumus.

2. Finanšu vienības izveido attiecīgus procesus, lai nodrošinātu ar IKT saistītu incidentu konsekventu un integrētu uzraudzību, apstrādi un turpmāko kontroli, lai pārliecinātos, ka ir identificēti pamatā esošie cēloņi un tie novērsti, lai šādi incidenti neatkārtotos.

3. Šā panta 1. punktā minētajā ar IKT saistītu incidentu pārvaldības procesā:

   (a) izveido procedūras ar IKT saistītu incidentu identificēšanai, izsekošanai, reģistrēšanai, kategorizācijai un iedalīšanai atbilstīgi to prioritātei, kā arī skarto pakalpojumu nopietnībai un būtiskumam saskaņā ar 16. panta 1. punktā minētajiem kritērijiem;

   (b) iedala funkcijas un atbildību, kas jāiedarbina attiecībā uz dažādiem ar IKT saistītiem incidentu veidiem un scenārijiem;

   (c) saskaņā ar 13. pantu izstrādā plānus, kā sazināties ar personālu, ārējām ieinteresētajām personām un plašsaziņas līdzekļiem un kā informēt klientus, īstenot iekšējās eskalācijas procedūras, tostarp saistībā ar klientu sūdzībām par IKT jautājumiem, kā arī informācijas sniegšanai finanšu vienībām, kas attiecīgi darbojas kā darījumu partneri;

   (d) nodrošina, ka par būtiskiem ar IKT saistītiem incidentiem tiek ziņots attiecīgajai augstākajai vadībai, kā arī vadības struktūra tiek informēta par būtiskiem ar IKT saistītiem incidentiem, skaidrojot to ietekmi, reaģēšanu un papildu kontroli, kas tiek noteikta ar IKT saistītu incidentu rezultātā;

   (e) izveido ar IKT saistītu incidentu reaģēšanas procedūras, lai mazinātu ietekmi un nodrošinātu to, ka pakalpojumi laikus kļūst operatīvi un drošāki.

16. pants

Ar IKT saistītu incidentu klasifikācija

1. Finanšu vienības klasificē ar IKT saistītus incidentus un nosaka to ietekmi, pamatojoties uz šādiem kritērijiem:

   (a) lietotāju vai finanšu darījumu partneru skaits, ko ir skāris ar IKT saistītā incidenta izraisītais pārtraukums, kā arī tas, vai ar IKT saistītais incidents ir ietekmējis reputāciju;

   (b) ar IKT saistītā incidenta ilgums, ieskaitot pakalpojuma nepieejamību;

(c) ģeogrāfiskā izplatība attiecībā uz jomām, ko skāris ar IKT saistītais incidents, jo īpaši, ja tas skar vairāk nekā divas dalībvalstis;

(d) ar IKT saistītā incidenta radītie datu zudumi, piemēram, integritātes zaudēšana, konfidencialitātes zaudēšana vai pieejamības zaudēšana;

(e) cik būtiski ar IKT saistītais incidents ietekmējis finanšu vienības IKT sistēmas;

(f) ietekmēto pakalpojumu, ieskaitot finanšu vienības darījumus un operācijas, būtiskums;

(g) ar IKT saistītā incidenta absolūtā un relatīvā ekonomiskā ietekme.

2. EUI ar EUI Apvienotās komitejas ("Apvienotā komiteja") starpniecību un pēc apspriešanās ar Eiropas Centrālo banku (ECB) un *ENISA* izstrādā kopēju regulatīvo tehnisko standartu projektus, tajā sīkāk nosakot:

(a) 1. punktā paredzētos kritērijus, ieskaitot būtiskuma robežvērtības, pēc kā noteikt būtiskus ar IKT saistītus incidentus, kam piemēro 17. panta 1. punktā paredzēto ziņošanas pienākumu;

(b) kritērijus, ko piemēro kompetentās iestādes, lai izvērtētu būtisku ar IKT saistītu incidentu nozīmi citu dalībvalstu jurisdikcijām, kā arī sīkāku informāciju ar IKT saistītu incidentu ziņojumos, kas tiek koplietota ar citām kompetentajām iestādēm saskaņā 17. panta 5. un 6. punktu.

3. Izstrādājot 2. punktā minēto kopējo regulatīvo tehnisko standartu projektus, EUI ņem vērā starptautiskos standartus, kā arī *ENISA* izstrādātās un publicētās specifikācijas, tajā skaitā attiecīgos gadījumos — citu ekonomikas nozaru specifikācijas.

EUI iesniedz Komisijai minēto kopējo regulatīvo tehnisko standartu projektus līdz [*PB: ievietot datumu, kas ir vienu gadu pēc spēkā stāšanās dienas*].

Komisijai tiek deleģētas pilnvaras papildināt šo regulu, pieņemot 2. punktā minētos regulatīvos tehniskos standartus attiecīgi saskaņā ar 10.–14. pantu Regulā (ES) Nr. 1093/2010, Regulā (ES) Nr. 1094/2010 un Regulā (ES) Nr. 1095/2010 .

17. pants

Ziņošana par būtiskiem ar IKT saistītiem incidentiem

1. Finanšu vienības par būtiskiem ar IKT saistītiem incidentiem ziņo 41. pantā minētajai attiecīgajai kompetentajai iestādei, ievērojot 3. punktā paredzēto termiņu.

Piemērojot šā punkta pirmo daļu, finanšu vienības pēc visas attiecīgās informācijas ievākšanas un analīzes sagatavo incidenta ziņojumu, izmantojot 18. pantā minēto veidni, un iesniedz to kompetentajai iestādei.

Ziņojumā ietver visu informāciju, kas nepieciešama kompetentajai iestādei, lai noteiktu būtiskā ar IKT saistītā incidenta nozīmīgumu un izvērtētu iespējamo pārrobežu ietekmi.

2. Ja būtisks ar IKT saistīts incidents ir vai varētu būt ietekmējis pakalpojuma lietotāju un klientu finanšu intereses, finanšu vienības bez nepamatotas kavēšanās informē pakalpojuma lietotājus un klientus par būtisko ar IKT saistīto incidentu un, cik ātri vien iespējams, informē tos par visiem pasākumiem, kas veikti, lai mazinātu šā incidenta nelabvēlīgo ietekmi.

3. Finanšu vienības 41. pantā minētajai kompetentajai iestādei iesniedz:

(a) sākotnēju ziņojumu bez nepamatotas kavēšanās, bet ne vēlāk kā līdz darbdienas beigām vai, ja būtisks ar IKT saistīts incidents noticis vēlāk nekā divas stundas pirms darbdienas beigām, — ne vēlāk kā četru stundu laikā pēc nākamās darbdienas sākuma, vai, ja ziņošanas kanāli nav pieejami, — tiklīdz tie kļuvuši pieejami;

(b) starpposma ziņojumu ne vēlāk kā vienu nedēļu pēc a) apakšpunktā minētā sākotnējā ziņojuma, kam vajadzības gadījumā seko atjaunināti paziņojumi ikreiz, kad ir pieejams attiecīgs statusa atjauninājums, kā arī pēc kompetentās iestādes konkrēta pieprasījuma;

(c) gala ziņojumu, kad ir pabeigta pamatcēloņu analīze un neatkarīgi no tā, vai mazināšanas pasākumi jau ir vai nav ieviesti, un kad ir pieejami faktiskie ietekmes rādītāji, ar ko aizstāt aplēses, bet ne vēlāk kā pēc mēneša no sākotnējā ziņojuma nosūtīšanas.

4. Finanšu vienības šajā pantā noteikto ziņošanas pienākumu var deleģēt trešās puses pakalpojumu sniedzējam vienīgi pēc tam, kad deleģēšanu atļāvusi attiecīgā 41. pantā minētā kompetentā iestāde.

5. Kad kompetentā iestāde ir saņēmusi 1. punktā minēto paziņojumu, tā bez liekas kavēšanās sniedz attiecīgo informāciju par incidentu:

(a) attiecīgā gadījumā — EBI, EVTI vai EAAPI;

(b) par šīs regulas 2. panta 1. punkta a), b) un c) apakšpunktā minētajām finanšu vienībām attiecīgā gadījumā — ECB; kā arī

(c) vienotajam kontaktpunktam, kas izraudzīts saskaņā ar Direktīvas (ES) 2016/1148 8. pantu.

6. EBI, EVTI vai EAAPI un ECB novērtē būtisko ar IKT saistīto incidentu nozīmīgumu citām attiecīgajām valsts iestādēm un par to tās attiecīgi informē iespējami īsā laikā. ECB paziņo Eiropas Centrālo banku sistēmas locekļiem par jautājumiem, kuri attiecas uz maksājumu sistēmu. Pamatojoties uz minēto paziņojumu, kompetentās iestādes vajadzības gadījumā veic visus pasākumus, kas nepieciešami, lai īstermiņā aizsargātu finanšu sistēmas drošību.

18. pants

Ziņojumu satura un veidņu saskaņošana

1. EUI, izmantojot Apvienoto komiteju un apspriežoties ar *ENISA* un ECB, izstrādā:

(a) kopējo regulatīvo tehnisko standartu projektus, ar ko:

(1) nosaka par būtiskiem ar IKT saistītiem incidentiem iesniegto ziņojumu saturu;

(2) sīkāk precizē nosacījumus, saskaņā ar kuriem finanšu vienības pēc kompetentās iestādes iepriekšēja apstiprinājuma var deleģēt trešo personu, kas sniedz pakalpojumus, šajā nodaļā izklāstītos ziņošanas pienākumus;

(b) kopējo īstenošanas tehnisko standartu projektus, ar ko nosaka standarta veidlapas, veidnes un procedūras, kā finanšu vienības ziņo par būtisku ar IKT saistītu incidentu.

EUI iesniedz Komisijai 1. punkta a) apakšpunktā minēto kopējo regulatīvo tehnisko standartu projektus un 1. punkta b) apakšpunktā minēto kopējo īstenošanas tehnisko standartu projektus līdz xx 202x [*PB*: *ievietot datumu, kas ir vienu gadu pēc spēkā stāšanās dienas*].

Komisijai tiek deleģētas pilnvaras papildināt šo regulu, pieņemot 1. punkta a) apakšpunktā minētos kopējos regulatīvos tehniskos standartus attiecīgi saskaņā ar 10.–14. pantu Regulā (ES) Nr. 1093/2010, Regulā (ES) Nr. 1095/2010 un Regulā (ES) Nr. 1094/2010.

Komisijai tiek deleģētas pilnvaras pieņemt 1. punkta b) apakšpunktā minētos kopējos īstenošanas tehniskos standartus attiecīgi saskaņā ar Regulas (ES) Nr. 1093/2010, (ES) Nr. 1095/2010 un (ES) Nr. 1094/2010 15. pantu.

19. pants

Centralizēta ziņošana par būtiskiem ar IKT saistītiem incidentiem

1. EUI ar Apvienotās komitejas starpniecību un apspriežoties ar ECB un *ENISA*, sagatavo kopīgu ziņojumu, kurā izvērtē iespēju turpināt centralizēt ziņošanu par incidentiem, izveidojot vienotu ES centrmezglu finanšu vienību ziņojumiem par būtiskiem ar IKT saistītiem incidentiem. Ziņojumā aplūko veidus, kā atvieglot ar IKT saistītu incidentu paziņošanas plūsmu, samazināt ar to saistītās izmaksas un izmantot tematiskās analīzes, lai uzlabotu uzraudzības konverģenci.

2. Šā panta 1. punktā minētajā ziņojumā ir vismaz šādi elementi:

   (a) priekšnoteikumi šāda ES centrmezgla izveidei;

   (b) ieguvumi, ierobežojumi un iespējamie riski;

   (c) darbības vadības elementi;

   (d) dalības nosacījumi;

   (e) kārtība, kādā finanšu vienības un valstu kompetentās iestādes var piekļūt ES centrmezglam;

   (f) provizorisks novērtējums par finansiālajām izmaksām, kas saistītas ar ES centrmezgla atbalsta darbības platformas izveidi, tostarp tai nepieciešamajām zināšanām.

3. EUI iesniedz 1. punktā minēto ziņojumu Komisijai, Eiropas Parlamentam un Padomei līdz xx 202x [*OV*: *ievietot datumu, kas ir trīs gadus pēc spēkā stāšanās dienas*].

20. pants

Uzrauga atgriezeniskā saite

1. Saņemot 17. panta 1. punktā minēto ziņojumu, kompetentā iestāde apstiprina paziņojuma saņemšanu un pēc iespējas ātrāk sniedz finanšu vienībai visu vajadzīgo atgriezenisko saiti vai norādījumus, jo īpaši, lai apspriestu tiesiskās aizsardzības līdzekļus vienības līmenī vai veidus, kā samazināt nelabvēlīgo ietekmi pa nozarēm.

2. EUI ar Apvienotās komitejas starpniecību katru gadu sniedz anonimizētu un apkopotu informāciju par IKT incidentu paziņojumiem, kas saņemti no kompetentajām iestādēm, izklāstot vismaz ar IKT saistīto būtisko incidentu skaitu, to

būtību, ietekmi uz finanšu vienību vai klientu darbību, izmaksas un veiktos korektīvos pasākumus.

EUI izdod brīdinājumus un sagatavo augsta līmeņa statistiku, lai atbalstītu IKT apdraudējumu un neaizskaramības novērtējumus.

IV NODAĻA

DIGITĀLĀS DARBĪBAS NOTURĪBAS TESTĒŠANA

21. pants

Vispārējās prasības digitālās darbības noturības testu veikšanai

1. Lai novērtētu gatavību ar IKT saistītiem incidentiem vai identificētu digitālās darbības noturības vājās vietas, trūkumus vai nepilnības un nekavējoties īstenotu korektīvos pasākumus, finanšu vienības, pienācīgi ņemot vērā to lielumu, darījumdarbības un riska profilus, izveido, uztur un pārskata stabilu un visaptverošu digitālās darbības noturības testēšanas programmu kā 5. pantā minētās IKT riska pārvaldības sistēmas neatņemamu daļu.

2. Digitālās darbības noturības testēšanas programma ietver virkni novērtējumu, testu, metodiku, prakses un rīku, ko piemēro saskaņā ar 22. un 23. panta noteikumiem.

3. Veicot šā panta 1. punktā minēto digitālās darbības noturības testēšanas programmu, finanšu vienības ievēro uz risku balstītu pieeju, ņemot vērā IKT risku mainīgo ainu, visus īpašos riskus, kuriem finanšu vienība ir vai varētu būt pakļauta, informācijas aktīvu un sniegto pakalpojumu kritisko svarīgumu, kā arī jebkuru citu faktoru, ko finanšu vienība uzskata par nozīmīgu.

4. Finanšu vienības nodrošina, ka testēšanu veic neatkarīgas personas, kas var būt iekšējas vai ārējas.

5. Finanšu vienības izveido procedūras un politikas pasākumus, lai noteiktu par prioritārām, klasificētu un novērstu visas problēmas, kuru pastāvēšana ir atzīta visā testu veikšanas procesā, un izveido iekšējās validēšanas metodiku, lai pārliecinātos, ka visas konstatētās vājās vietas, trūkumi vai nepilnības ir pilnībā novērsti.

6. Finanšu vienības testē visas kritiski svarīgās IKT sistēmas un lietojumprogrammas vismaz reizi gadā.

22. pants

IKT rīku un sistēmu testēšana

1. Regulas 21. pantā minētā digitālās darbības noturības testēšanas programma paredz veikt pilnu atbilstīgu testu loku, tostarp neaizskaramības novērtējumus un skenēšanu, atklātā pirmkoda analīzi, tīkla drošības novērtējumus, nepilnību analīzi, fiziskās drošības pārbaudes, anketas un skenēšanas programmatūras risinājumus, pirmkodu pārskatīšanu (ja iespējams), uz scenārijiem balstītus testus, saderības testēšanu, veiktspējas testēšanu, testēšanu "no gala līdz galam" vai ielaušanās testēšanu.

2. Regulas 2. panta 1. punkta f) un g) apakšpunktā minētās finanšu vienības veic neaizskaramības novērtējumu, pirms tiek (atkārtoti) ieviesti jauni vai esoši pakalpojumi, kas atbalsta finanšu vienības kritiski svarīgās funkcijas, lietojumprogrammas un infrastruktūras komponentus.

23. pants

IKT rīku, sistēmu un procesu padziļināta testēšana, balstoties uz draudu vadītu ielaušanās testēšanu

1. Saskaņā ar 4. punktu identificētās finanšu vienības vismaz reizi trijos gados veic padziļinātu testēšanu, izmantojot draudu vadītu ielaušanās testēšanu.

2. Draudu vadīta ielaušanās testēšana aptver vismaz finanšu vienības kritiski svarīgās funkcijas un pakalpojumus, un to veic aktīvā izstrādes sistēmā, kas atbalsta šīs funkcijas. Draudu vadītas ielaušanās testēšanas precīzu jomu, balstoties uz kritiski svarīgu funkciju un pakalpojumu novērtējumu, nosaka finanšu vienības un validē kompetentās iestādes.

   Pirmās daļas vajadzībām finanšu vienības identificē visus attiecīgos pamatā esošos IKT procesus, sistēmas un tehnoloģijas, kas atbalsta kritiski svarīgas funkcijas un pakalpojumus, ieskaitot funkcijas un pakalpojumus, kas uzticēti ārpakalpojumā vai par ko noslēgts līgums ar trešām personām, kas sniedz IKT pakalpojumus.

   Ja draudu vadīta ielaušanās testēšana aptver trešās personas, kas sniedz IKT pakalpojumus, finanšu vienība veic nepieciešamos pasākumus, lai nodrošinātu šo pakalpojumu sniedzēju piedalīšanos.

   Finanšu vienības piemēro efektīvas riska pārvaldības kontroles, lai mazinātu risku, ka varētu tikt ietekmēti pašas finanšu vienības, tās darījumu partneru vai finanšu nozares dati, bojāti aktīvi vai traucēti kritiski svarīgi pakalpojumi vai darbības.

   Pēc testa beigām, kad apstiprināti ziņojumi un sanācijas plāni, finanšu vienība un ārējie testētāji iesniedz kompetentajai iestādei dokumentus, kas apstiprina, ka draudu vadītā ielaušanās testēšana ir veikta atbilstīgi prasībām. Kompetentās iestādes validē dokumentus un izsniedz apliecinājumu.

3. Finanšu vienības draudu vadītas ielaušanās testēšanas veikšanai noslēdz līgumus ar testētājiem saskaņā ar 24. pantu.

   Kompetentās iestādes identificē finanšu vienības, kam jāveic draudu vadīta ielaušanās testēšana, proporcionāli finanšu vienības lielumam, mērogam, darbībai un kopējam riska profilam, balstoties uz šādu faktoru izvērtējumu:

   (a) ar ietekmi saistīti faktori, jo īpaši finanšu vienības sniegto pakalpojumu un darbību kritiskais svarīgums;

   (b) iespējamās bažas par finanšu stabilitāti, attiecīgā gadījumā ieskaitot finanšu vienības sistēmiskumu valsts vai Savienības līmenī;

   (c) finanšu vienības konkrētais IKT riska profils, IKT gatavības līmenis vai attiecīgās tehnoloģijas īpašības.

4. EBI, EVTI un EAAPI pēc apspriešanās ar ECB un ņemot vērā attiecīgo regulējumu Savienībā, ko piemēro izlūkdatu vadītas ielaušanās testos, izstrādā regulatīvo tehnisko standartu projektus, lai sīkāk noteiktu:

   (a) šā panta 6. punkta piemērošanas vajadzībām izmantotos kritērijus;

   (b) prasības attiecībā uz:

      (a) šā panta 2. punktā minēto draudu vadītas ielaušanās testu darbības jomu;

      (b) testēšanas metodiku un pieeju, ko ievēro katrā testēšanas procesa konkrētajā posmā;

(c) testēšanas rezultātu, slēgšanas un kļūdu novēršanas posmus;

(c) tādas uzraudzības sadarbības veidu, kas vajadzīga, lai īstenotu draudu vadītu ielaušanās testēšanu saistībā ar finanšu vienībām, kuras darbojas vairāk nekā vienā dalībvalstī, lai nodrošinātu pienācīgu uzraudzības iesaisti un elastīgu īstenošanu nolūkā ņemt vērā finanšu apakšnozaru vai vietējo finanšu tirgu īpatnības.

EUI iesniedz Komisijai minēto regulatīvo tehnisko standartu projektus līdz [*OV: ievietot datumu, kas ir divus mēnešus pirms spēkā stāšanās dienas*].

Komisijai tiek deleģētas pilnvaras papildināt šo regulu, pieņemot otrajā daļā minētos regulatīvos tehniskos standartus attiecīgi saskaņā ar 10.–14. pantu Regulā (ES) Nr. 1093/2010, Regulā (ES) Nr. 1095/2010 un Regulā (ES) Nr. 1094/2010.

24. pants

Prasības testētājiem

1. Finanšu vienības draudu vadītas ielaušanās testēšanai izmanto tikai testētājus:

(a) kam ir visaugstākā piemērotība un reputācija;

(b) kam ir tehniskās un organizēšanas spējas, kā arī tie ir apliecinājuši, ka tiem ir īpaša zinātība par draudu izlūkdatiem, ielaušanās testēšanu vai sarkanās komandas testēšanu;

(c) ko ir sertificējusi dalībvalsts akreditācijas struktūra vai kas ievēro oficiālus rīcības kodeksus vai ētikas regulējumu;

(d) kas kā ārējie testētāji sniedz neatkarīgu apliecinājumu vai revīzijas ziņojumu saistībā ar tādu risku stabilu pārvaldību, kas ir saistīti ar draudu vadītu ielaušanās testu izpildi, tostarp finanšu vienības konfidenciālās informācijas pienācīgu aizsardzību un finanšu vienības darījumdarbības risku atlīdzināšanu;

(e) kam kā ārējiem testētājiem ir pienācīgs un pilnīgs attiecīgas profesionālās apdrošināšanas segums, tostarp pret ļaunprātīgas rīcības un nolaidības riskiem.

2. Finanšu vienības nodrošina, ka ar ārējiem testētājiem noslēgtajos nolīgumos ir obligāti noteikts stabili pārvaldīt draudu vadītas ielaušanās rezultātus un ka to apstrāde, ieskaitot izveidošanu, projekta izstrādi, glabāšanu, apkopošanu, ziņošanu, paziņošanu vai iznīcināšanu, nerada riskus finanšu vienībai.

V NODAĻA

AR TREŠO PERSONU SAISTĪTA IKT RISKA PĀRVALDĪBA

I IEDAĻA

AR TREŠO PERSONU SAISTĪTA IKT RISKA STABILAS PĀRVALDĪBAS PAMATPRINCIPI

25. pants

Vispārīgie principi

Finanšu vienības savās IKT riska pārvaldības sistēmā pārvalda ar trešo personu saistīto IKT risku kā IKT riska neatņemamu daļu saskaņā ar turpmāk izklāstītajiem principiem.

1. Finanšu vienības, kurām ir līgumiskas vienošanās par IKT pakalpojumu izmantošanu savas darījumdarbības veikšanai, nepārtraukti ir pilnībā atbildīgas par visu šajā regulā un piemērojamos finanšu pakalpojumu tiesību aktos noteikto saistību ievērošanu un izpildi.

2. Finanšu vienības īsteno ar trešo personu saistītā riska pārvaldību saskaņā ar proporcionalitātes principu, ņemot vērā:

   (a) ar IKT saistītu atkarību apmēru, sarežģītību un svarīgumu;

   (b) riskus, kuri rodas no līgumiskas vienošanās par IKT pakalpojumu sniegšanu, kas noslēgta ar trešām personām, kas sniedz IKT pakalpojumus, ņemot vērā attiecīgā pakalpojuma, procesa vai funkcijas kritisko svarīgumu vai svarīgumu un iespējamo ietekmi uz finanšu pakalpojumu un darbību nepārtrauktību un kvalitāti individuālā un grupas līmenī.

3. Finanšu vienības kā daļu no IKT riska pārvaldības sistēmas pieņem un regulāri pārskata ar trešo personu saistītā IKT riska stratēģiju, ņemot vērā 5. panta 9. punkta g) apakšpunktā minēto vairāku piegādātāju stratēģiju. Šajā stratēģijā ietver rīcībpolitiku attiecībā uz trešo personu, kas sniedz IKT pakalpojumus, sniegto IKT pakalpojumu izmantošanu, un to piemēro individuāli, kā arī attiecīgā gadījumā — subkonsolidēti un konsolidēti. Vadības struktūra regulāri pārskata riskus, kas identificēti attiecībā uz kritiski svarīgu vai svarīgu funkciju uzticēšanu ārpakalpojuma sniedzējiem.

4. Finanšu vienības IKT riska pārvaldības sistēmas ietvaros vienības līmenī, kā arī subkonsolidētajā un konsolidētajā līmenī uztur un atjaunina informācijas reģistru saistībā ar katru līgumisku vienošanos par izmantotajiem IKT pakalpojumiem, ko sniedz trešās personas.

   Pirmajā daļā minētās līgumiskās vienošanās attiecīgi dokumentē, nošķirot tās, kas attiecas uz kritiski svarīgām vai svarīgām funkcijām.

   Finanšu vienības vismaz reizi gadā sniedz kompetentajām iestādēm informāciju par jaunu pasākumu skaitu attiecībā uz IKT pakalpojumu izmantošanu, trešo personu, kas sniedz IKT pakalpojumus, kategorijām, līgumisku vienošanos veidiem un nodrošinātajiem pakalpojumiem un funkcijām.

Finanšu vienības pēc pieprasījuma dara kompetentajai iestādei pieejamu pilno informācijas reģistru vai pieprasīto informāciju, kā arī jebkādu informāciju, ko uzskata par nepieciešamu finanšu vienības efektīvas uzraudzības nodrošināšanai.

Finanšu vienības laikus informē kompetento iestādi par plānotu līgumu noslēgšanu par kritiski svarīgām vai svarīgām funkcijām, kā arī par to, ka funkcija ir kļuvusi par kritiski svarīgu vai svarīgu.

5. Finanšu vienības, pirms tās noslēdz līgumisku vienošanos par IKT pakalpojumu izmantošanu:

   (a) novērtē, vai līgumiskā vienošanās attiecas uz kritiski svarīgu vai svarīgu funkciju;

   (b) novērtē, vai ir izpildīti uzraudzības nosacījumi līguma slēgšanai;

   (c) identificē un novērtē visus būtiskos riskus saistībā ar līgumisko vienošanos, tostarp iespēju, ka šāda līgumiska vienošanās var sekmēt IKT koncentrācijas riska palielināšanos;

   (d) ar visu pienācīgo rūpību pārbauda iespējamās trešās personas, kas sniedz IKT pakalpojumus, un visos atlases un novērtēšanas procesos nodrošina, ka trešā persona, kas sniedz IKT pakalpojumus, ir piemērota;

   (e) identificē un novērtē interešu konfliktus, ko var izraisīt līgumiskā vienošanās.

6. Finanšu vienības var slēgt līgumiskas vienošanās tikai ar tādām trešām personām, kas sniedz IKT pakalpojumus, kuras atbilst augstiem, atbilstošiem un jaunākajiem informācijas drošības standartiem.

7. Īstenojot piekļuves, pārbaudes un revīzijas tiesības attiecībā uz trešo personu, kas sniedz IKT pakalpojumus, finanšu vienības, izmantojot uz risku balstītu pieeju, iepriekš nosaka revīziju un pārbaužu biežumu un revidējamās jomas, ievērojot vispārpieņemtus revīzijas standartus un atbilstīgi uzraudzības norādījumiem par šādu revīzijas standartu izmantošanu un iestrādāšanu.

   Ja līgumiska vienošanās ir ar augstu tehnoloģiskās sarežģītības līmeni, finanšu vienība pārbauda, vai revidentiem, neatkarīgi no tā, vai tie ir iekšēji revidenti, revidentu grupas vai ārējie revidenti, piemīt atbilstīgas prasmes un zināšanas, lai efektīvi veiktu attiecīgās revīzijas un novērtējumus.

8. Finanšu vienības nodrošina, ka līgumiskas vienošanās par IKT pakalpojumu izmantošanu tiek izbeigtas vismaz šādos gadījumos:

   (a) trešā persona, kas sniedz IKT pakalpojumus, pārkāpj piemērojamos tiesību aktus, noteikumus vai līguma noteikumus;

   (b) apstākļi, kuri identificēti visā ar trešo personu saistītā riska pārraudzībā un kurus uzskata par tādiem, kas var mainīt ar līgumisko vienošanos sniegto funkciju izpildi, tostarp būtiskas izmaiņas, kas ietekmē trešās personas, kas sniedz IKT pakalpojumus, struktūru vai situāciju;

   (c) pastāv apliecinātas trešās personas, kas sniedz IKT pakalpojumus, nepilnības vispārējā IKT riska pārvaldībā un jo īpaši attiecībā uz to, kā tas nodrošina konfidenciālu, personisku vai citādi sensitīvu datu vai konfidenciālas informācijas drošību un integritāti;

   (d) apstākļi, kad kompetentā iestāde attiecīgās līgumiskās vienošanās rezultātā vairs nevar efektīvi uzraudzīt finanšu vienību.

9. Finanšu vienības ievieš atkāpšanās stratēģijas, lai ņemtu vērā riskus, kas var rasties trešās personas, kas sniedz IKT pakalpojumus, līmenī, jo īpaši tā iespējamā saistību neizpilde, sniegto funkciju kvalitātes pasliktināšanās, jebkādi darījumdarbības traucējumi neatbilstošas vai nesekmīgas pakalpojumu sniegšanas dēļ, vai ar attiecīgās funkcijas pienācīgu un nepārtrauktu izvietošanu saistīta būtiska riska rašanās.

Finanšu vienības nodrošina, ka tās var atkāpties no līgumiskas vienošanās:

(a) netraucējot to darījumdarbībai;

(b) neierobežojot atbilstību regulatīvajām prasībām;

(c) nekaitējot klientiem sniegto pakalpojumu nepārtrauktībai un kvalitātei.

Atkāpšanās plāni ir visaptveroši, dokumentēti un attiecīgos gadījumos — pietiekami testēti.

Finanšu vienības identificē alternatīvus risinājumus un izstrādā pārejas plānus, kas tām ļauj ar līgumu noteiktās funkcijas un attiecīgos datus pārvietot no trešās personas, kas sniedz IKT pakalpojumus, un droši un vienoti nodot tos citiem pakalpojumu sniedzējiem vai atkārtoti iekļaut vienības iekšienē.

Finanšu vienības veic attiecīgus ārkārtas pasākumus, lai nodrošinātu darbības nepārtrauktību visos pirmajā daļā minētajos gadījumos.

10. EUI ar Apvienotās komitejas starpniecību izstrādā īstenošanas tehnisko standartu projektus, lai izveidotu standarta veidnes 4. punktā minētā informācijas reģistra vajadzībām.

EUI iesniedz Komisijai minēto īstenošanas tehnisko standartu projektus līdz [*OV: ievietot datumu, kas ir vienu gadu pēc regulas spēkā stāšanās dienas*].

Komisijai tiek deleģētas pilnvaras pieņemt pirmajā daļā minētos īstenošanas tehniskos standartus attiecīgi saskaņā ar 10.–14. pantu Regulā (ES) Nr. 1093/2010, Regulā (ES) Nr. 1095/2010 un Regulā (ES) Nr. 1094/2010.

11. EUI ar Apvienotās komitejas starpniecību izstrādā regulatīvo standartu projektus:

(a) lai sīkāk precizētu 3. punktā minētās rīcībpolitikas detalizēto saturu saistībā ar līgumisko vienošanos par trešās personas, kas sniedz IKT pakalpojumus, sniegto IKT pakalpojumu izmantošanu, atsaucoties uz attiecīgās vienošanās par IKT pakalpojumu izmantošanu dzīves cikla galvenajiem posmiem;

(b) attiecībā uz informāciju, kas iekļaujama 4. punktā minētajā informācijas reģistrā.

EUI iesniedz Komisijai minēto regulatīvo tehnisko standartu projektus līdz [*PB: ievietot datumu, kas ir vienu gadu pēc spēkā stāšanās dienas*].

Komisijai tiek deleģētas pilnvaras papildināt šo regulu, pieņemot otrajā daļā minētos regulatīvos tehniskos standartus attiecīgi saskaņā ar 10.–14. pantu Regulā (ES) Nr. 1093/2010, Regulā (ES) Nr. 1095/2010 un Regulā (ES) Nr. 1094/2010.

26. pants

IKT koncentrācijas riska un ārpakalpojuma tālākas deleģēšanas sākotnējais novērtējums

1. Veicot 25. panta 5. punkta c) apakšpunktā minētā IKT koncentrācijas riska identificēšanu un novērtēšanu, finanšu vienības ņem vērā, vai līgumiskas vienošanās noslēgšana par IKT pakalpojumiem radītu kādas no šādām sekām:

   (a) līguma noslēgšana ar trešo personu, kas sniedz IKT pakalpojumus un kas nav viegli aizstājama; vai

   (b) pastāvētu vairākas līgumiskas vienošanās attiecībā uz IKT pakalpojumu sniegšanu ar tādu pašu trešo personu, kas sniedz IKT pakalpojumus, vai ar cieši saistītām trešām personām, kas sniedz IKT pakalpojumus.

   Finanšu vienības izvērtē izmaksas un ieguvumus no alternatīvu risinājumu izmantošanas, piemēram, dažādu trešo personu, kas sniedz IKT pakalpojumus, izmantošanas, ņemot vērā, vai un kā paredzētie risinājumi atbilst digitālās darbības noturības stratēģijā izklāstītajām darījumdarbības vajadzībām un mērķiem.

2. Ja līgumiskā vienošanās par IKT pakalpojumu izmantošanu ietver iespēju, ka trešā persona, kas sniedz IKT pakalpojumus, kritiski svarīgu vai svarīgu funkciju nodod tālāk ārpakalpojumā citām trešām personām, kas sniedz IKT pakalpojumus, finanšu vienības izvērtē ieguvumus un riskus, kas varētu rasties saistībā ar šādu tālāknodošanu ārpakalpojumā, jo īpaši, ja IKT apakšuzņēmējs ir reģistrēts trešā valstī.

   Ja līgumisko vienošanos par IKT pakalpojumu izmantošanu slēdz ar trešo personu, kas sniedz IKT pakalpojumus, kura ir reģistrēta trešā valstī, finanšu vienības apsver attiecīgus faktorus, kuru vidū ir vismaz:

   (a) datu aizsardzības ievērošana;

   (b) efektīva tiesību piemērošana;

   (c) maksātnespējas tiesību noteikumi, ko piemērotu, ja trešā persona, kas sniedz IKT pakalpojumus, bankrotētu;

   (d) ierobežojumi, kas varētu rasties saistībā ar finanšu vienības datu steidzamu atgūšanu.

   Finanšu vienības vērtē, vai un kā iespējamās garās vai sarežģītās apakšuzņēmēju ķēdes varētu ietekmēt to spēju pilnībā uzraudzīt ar līgumu nodotās funkcijas un kompetentās iestādes spēju šajā ziņā efektīvi uzraudzīt finanšu vienību.

27. pants

Svarīgākie līgumu noteikumi

1. Finanšu vienības un trešās personas, kas sniedz IKT pakalpojumus, tiesības un pienākumus sadala skaidri un noformulē rakstiski. Visu līgumu, kurā ir ietvertas pakalpojumu līmeņa vienošanās, dokumentē vienā rakstiskā dokumentā, kas ir pieejams pusēm papīra vai lejupielādējamā un piekļūstamā formātā.

2. Līgumiskas vienošanās par IKT pakalpojumu izmantošanu ietver vismaz:

   (a) visu trešās personas, kas sniedz IKT pakalpojumus, sniegto funkciju un pakalpojumu skaidru un pilnīgu aprakstu, tostarp norādot, vai ir atļauts kritiski

svarīgu vai svarīgu funkciju vai būtiskas tās daļas nodot apakšuzņēmējam un, ja jā — nosacījumus, ko piemēro nodošanai apakšuzņēmējam;

(b) ar līgumu vai apakšuzņēmuma līgumu nodoto funkciju un pakalpojumu izpildes un datu apstrādes vietu, ieskaitot to glabāšanas vietu, kā arī prasību trešai personai, kas sniedz IKT pakalpojumus, paziņot finanšu vienībai, ja tā plāno šīs vietas mainīt;

(c) noteikumus par finanšu vienības apstrādāto personas datu un datu, kas nav personas dati, piekļūstamību, pieejamību, integritāti, drošību un aizsardzību, kā arī par piekļuvi šiem datiem, to atgūšanu un atgriešanu viegli pieejamā formātā trešās personas, kas sniedz IKT pakalpojumus, maksātnespējas, noregulējuma vai darījumdarbības izbeigšanas gadījumā;

(d) pilnīgus pakalpojumu līmeņa aprakstus, tostarp to atjauninājumus un pārskatīšanu, kā arī precīzus kvantitatīvus un kvalitatīvus darbības mērķus saskaņotajos pakalpojumu līmeņos, lai ļautu finanšu vienībai veikt efektīvu uzraudzību un bez liekas kavēšanās dotu iespēju veikt atbilstīgus koriģējošus pasākumus, ja netiek ievēroti saskaņotie pakalpojumu līmeņi;

(e) trešai personai, kas sniedz IKT pakalpojumus, saistošos paziņošanas termiņus un ziņošanas pienākumus attiecībā pret finanšu vienību, tostarp paziņošanu par jebkādu notikumu attīstību, kas varētu būtiski ietekmēt trešās personas, kas sniedz IKT pakalpojumus, spēju efektīvi veikt kritiski svarīgās vai svarīgās funkcijas atbilstīgi saskaņotajiem pakalpojumu līmeņiem;

(f) trešās personas, kas sniedz IKT pakalpojumus, pienākumu IKT incidenta gadījumā sniegt palīdzību bez papildu izmaksām vai par iepriekš noteiktu maksu;

(g) prasības trešai personai, kas sniedz IKT pakalpojumus, īstenot un pārbaudīt darījumdarbības ārkārtas situāciju plānus un ieviest IKT drošības pasākumus, instrumentus un politikas pasākumus, kas pienācīgi garantē pakalpojumu drošu sniegšanu finanšu vienībai saskaņā ar tās normatīvo regulējumu;

(h) tiesības pastāvīgi uzraudzīt trešās personas, kas sniedz IKT pakalpojumus, veikto izpildi, kas ietver:

i) finanšu vienības vai ieceltas trešās personas tiesības piekļūt, pārbaudīt un veikt revīziju, kā arī tiesības izgatavot attiecīgo dokumentu kopijas, kuru efektīvu īstenošanu nekavē un neierobežo citas līgumiskas vienošanās vai īstenošanas politika;

ii) tiesības vienoties par alternatīviem garantijas līmeņiem, ja tiek skartas citu klientu tiesības;

iii) apņemšanos pilnībā sadarboties finanšu vienības veiktajās pārbaudēs uz vietas un sīkāku informāciju par attālināto revīziju apjomu, kārtību un biežumu;

(i) trešās personas, kas sniedz IKT pakalpojumus, pienākumu pilnībā sadarboties ar finanšu vienības kompetentajām iestādēm un noregulējuma iestādēm, tostarp to ieceltajām personām;

(j) izbeigšanas tiesības un ar to saistītos minimālos termiņus, kādos jāpaziņo par līguma izbeigšanu, kas atbilst kompetento iestāžu gaidām;

(k) atkāpšanās stratēģijas, jo īpaši obligāta piemērota pārejas perioda noteikšanu:

(a) kuras laikā trešā persona, kas sniedz IKT pakalpojumus, turpinās nodrošināt attiecīgās funkcijas vai pakalpojumus nolūkā samazināt finanšu vienības darbības traucējumu risku;

(b) kas ļauj finanšu vienībai pāriet pie citas trešās personas, kas sniedz IKT pakalpojumus, vai pāriet uz risinājumiem vienības telpās, kas atbilst sniegtā pakalpojuma sarežģītībai.

3. Sarunās par līgumisku vienošanos finanšu vienības un trešās personas, kas sniedz IKT pakalpojumus, apsver iespēju izmantot konkrētiem pakalpojumiem izstrādātas līguma standartklauzulas.

4. EUI ar Apvienotās komitejas starpniecību izstrādā regulatīvo tehnisko standartu projektus, lai sīkāk precizētu elementus, ko finanšu vienībai nepieciešams noteikt un novērtēt, uzticot ārpakalpojuma sniedzējam kritiski svarīgas vai svarīgas funkcijas, lai pienācīgi īstenotu 2. punkta a) apakšpunkta noteikumus.

EUI iesniedz Komisijai minēto regulatīvo tehnisko standartu projektus līdz [*OV: ievietot datumu, kas ir vienu gadu pēc spēkā stāšanās dienas*].

Komisijai tiek deleģētas pilnvaras papildināt šo regulu, pieņemot pirmajā daļā minētos regulatīvos tehniskos standartus attiecīgi saskaņā ar 10.–14. pantu Regulā (ES) Nr. 1093/2010, Regulā (ES) Nr. 1095/2010 un Regulā (ES) Nr. 1094/2010.

II IEDAĻA

KRITISKU SVARĪGU TREŠO PERSONU, KAS SNIEDZ IKT PAKALPOJUMUS, PĀRRAUDZĪBAS SISTĒMA

28. pants

Kritisku svarīgu trešo personu, kas sniedz IKT pakalpojumus, izraudzīšanās

1. EUI ar Apvienotās komitejas starpniecību un pēc saskaņā ar 29. panta 1. punktu izveidotā Pārraudzības foruma ieteikuma:

(a) izraugās trešās personas, kas sniedz IKT pakalpojumus, kuras ir kritiski svarīgas finanšu vienībām, ņemot vērā 2. punktā noteiktos kritērijus;

(b) EBI, EVTI vai EAAPI ieceļ par galveno pārraugu katrai kritiski svarīgai trešai personai, kas sniedz IKT pakalpojumus, atkarībā no tā, vai finanšu vienību, kas izmanto IKT pakalpojumu, ko sniedz šī kritiski svarīgā trešā persona, un uz ko attiecas attiecīgi viena no Regulām (ES) Nr. 1093/2010 (ES), Nr. 1094/2010 vai (ES) Nr. 1095/2010, aktīvu kopējā vērtība veido vairāk nekā pusi no visu to finanšu vienību kopējo aktīvu vērtības, kuras izmanto kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, ko apliecina šo finanšu vienību konsolidētās bilances vai, ja bilances nav konsolidētas — atsevišķas bilances.

2. Šā panta 1. punkta a) apakšpunktā minētās izraudzīšanās pamatā ir visi šādi kritēriji:

(a) sistēmiskā ietekme uz finanšu pakalpojumu sniegšanas stabilitāti, nepārtrauktību vai kvalitāti gadījumā, ja attiecīgajai trešai personai, kas sniedz IKT pakalpojumus, iestātos plaši darbības traucējumi, kuru dēļ tā nespētu sniegt savus pakalpojumus, ņemot vērā to finanšu vienību skaitu, kurām attiecīgā trešā persona sniedz IKT pakalpojumus;

(b) finanšu vienību, kas paļaujas uz attiecīgo trešo personu, kas sniedz IKT pakalpojumus, sistēmiskais raksturs vai nozīme, ko novērtē saskaņā ar šādiem parametriem:

i) globālo sistēmiski nozīmīgo iestāžu (G-SNI) vai citu sistēmiski nozīmīgu iestāžu (C-SNI) skaits, kas paļaujas uz attiecīgo trešo personu, kas sniedz IKT pakalpojumus;

ii) iepriekš i) apakšpunktā minēto G-SNI vai C-SNI un citu finanšu vienību savstarpējā atkarība, tostarp situācijas, kad G-SNI vai C-SNI sniedz finanšu infrastruktūras pakalpojumus citām finanšu vienībām;

(c) finanšu vienību paļaušanās uz attiecīgās trešās personas, kas sniedz IKT pakalpojumus, sniegtajiem pakalpojumiem saistībā ar tādu finanšu vienību kritiski svarīgām vai svarīgām funkcijām, kurās galu galā ir iesaistīta viena un tā pati trešā persona, kas sniedz IKT pakalpojumus, neatkarīgi no tā, vai finanšu vienības šos pakalpojumus izmanto tieši vai netieši, izmantojot apakšuzņēmuma līgumus;

(d) trešās personas, kas sniedz IKT pakalpojumus, aizstājamības pakāpe, ņemot vērā šādus parametrus:

i) reālu alternatīvu trūkums, pat daļējs, ņemot vērā konkrētā tirgū strādājošo trešo personu, kas sniedz IKT pakalpojumus, ierobežoto skaitu vai attiecīgās trešās personas, kas sniedz IKT pakalpojumus, tirgus daļu, vai attiecīgo tehnisko sarežģītību vai komplicētību, tostarp attiecībā uz jebkuru patentētu tehnoloģiju, vai trešās personas, kas sniedz IKT pakalpojumus, organizācijas vai darbības specifiku;

ii) grūtības daļēji vai pilnībā migrēt attiecīgos datus un darba slodzes no attiecīgās trešās personas, kas sniedz IKT pakalpojumus, pie citas, ko rada vai nu būtiskas finansiālās izmaksas, laika vai citu resursu patēriņš, ko varētu radīt migrācijas process, vai palielināts IKT risks vai cits operacionālais risks, kam finanšu vienība var tikt pakļauta, ja tā veiktu šādu migrēšanu;

(e) to dalībvalstu skaits, kurās IKT pakalpojumus sniedz attiecīgā trešā persona;

(f) to dalībvalstu skaits, kurās darbojas finanšu vienības, kas izmanto IKT pakalpojumus, ko sniedz attiecīgā trešā persona.

3. Komisija saskaņā ar 50. pantu ir pilnvarota pieņemt deleģētos aktus, ar ko papildina 2. punktā minētos kritērijus.

4. Šā panta 1. punkta a) apakšpunktā minēto izraudzīšanās mehānismu neizmanto, kamēr Komisija saskaņā ar 3. punktu nav pieņēmusi deleģēto aktu.

5. Šā panta 1. punkta a) apakšpunktā minēto izraudzīšanās mehānismu nepiemēro attiecībā uz trešām personām, kas sniedz IKT pakalpojumus, kurām piemēro Līguma par Eiropas Savienības darbību 127. panta 2. punktā minēto uzdevumu atbalstam izveidotās pārraudzības sistēmas.

6. EUI ar Apvienotās komitejas starpniecību nosaka, publicē un katru gadu atjaunina Savienības līmeņa kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, sarakstu.

7. Šā panta 1. punkta a) apakšpunkta mērķiem kompetentās iestādes katru gadu apkopotā veidā nosūta 25. panta 4. punktā minētos ziņojumus saskaņā ar 29. pantu

izveidotajam Pārraudzības forumam. Pārraudzības forums izvērtē finanšu vienību atkarību no trešām personām, kas sniedz IKT pakalpojumus, balstoties uz informāciju, kas saņemta no kompetentajām iestādēm.

8. Trešās personas, kas sniedz IKT pakalpojumus, kuras nav iekļautas 6. punktā minētajā sarakstā, var pieprasīt, lai tās iekļauj šajā sarakstā.

Pirmās daļas vajadzībām trešā persona, kas sniedz IKT pakalpojumus, iesniedz argumentētu pieteikumu EBI, EVTI vai EAAPI, kas ar Apvienotās komitejas starpniecību lemj, vai iekļaut trešo personu, kas sniedz IKT pakalpojumus, sarakstā saskaņā ar 1. punkta a) apakšpunktu.

Otrajā daļā minēto lēmumu pieņem un par to paziņo trešai personai, kas sniedz IKT pakalpojumus, sešu mēnešu laikā no pieteikuma saņemšanas.

9. Finanšu vienības neizmanto trešā valstī reģistrētu trešo personu, kas sniedz IKT pakalpojumus, kura būtu izraudzīta kā kritiski svarīga saskaņā ar 1. punkta a) apakšpunktu, ja tā būtu reģistrēta Savienībā.

29. pants

Pārraudzības sistēmas struktūra

1. Apvienotā komiteja saskaņā ar Regulas (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010 57. pantu izveido Pārraudzības forumu kā apakškomiteju, lai tā atbalstītu 28. panta 1. punkta b) apakšpunktā minēto Apvienotās komitejas un galvenā pārrauga darbību ar trešo personu saistīta IKT riska jomā visās finanšu nozarēs. Pārraudzības forums izstrādā Apvienotās komitejas kopīgās nostājas projektus un kopīgos aktus šajā jomā.

Pārraudzības forums regulāri apspriež attiecīgo IKT risku un neaizskaramības notikumu attīstību un veicina vienotas pieejas izmantošanu, uzraugot ar trešo personu saistīto IKT risku Savienības mērogā.

2. Pārraudzības forums katru gadu veic visu kritiski svarīgo trešo personu, kas sniedz IKT pakalpojumus, veikto pārraudzības darbību rezultātu un konstatējumu kolektīvu novērtējumu un veicina koordinēšanas pasākumus, lai palielinātu finanšu vienību digitālās darbības noturību, veicinātu labāko praksi IKT koncentrācijas riska risināšanā un izpētītu atbildību mīkstinošus faktorus pārrobežu riska nodošanas gadījumos.

3. Pārraudzības forums saskaņā ar Regulas (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010 56. panta 1. punktu iesniedz visaptverošus kritiski svarīgo trešo personu, kas sniedz IKT pakalpojumus, kritērijus, ko Apvienotā komiteja pieņem kā EUI kopīgās nostājas.

4. Pārraudzības forumu veido EUI vadītāji un viens augsta līmeņa pārstāvis no attiecīgās kompetentās iestādes pašreizējā personāla katrā dalībvalstī. Katras EUI izpilddirektori un pa vienam pārstāvim no Eiropas Komisijas, ESRK, ECB un *ENISA* piedalās Pārraudzības forumā kā novērotāji.

5. EUI saskaņā ar Regulas (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010 16. pantu izdod pamatnostādnes par EUI un kompetento iestāžu sadarbību šīs iedaļas vajadzībām attiecībā uz sīki izstrādātām procedūrām un nosacījumiem, kas attiecas uz uzdevumu izpildi starp kompetentajām iestādēm un EUI, un informāciju par kompetentajām iestādēm nepieciešamās informācijas

apmaiņu, lai nodrošinātu turpmāku rīcību pēc ieteikumiem, ko galvenie pārraugi saskaņā ar 31. panta 1. punkta d) apakšpunktu adresējuši kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus.

6. Šajā iedaļā izklāstītās prasības neskar Direktīvas (ES) 2016/1148 un citu Savienības noteikumu par mākoņdatošanas pakalpojumu sniedzēju pārraudzību piemērošanu.

7. EUI ar Apvienotās komitejas starpniecību un pamatojoties uz Pārraudzības foruma veikto sagatavošanās darbu, katru gadu iesniedz Eiropas Parlamentam, Padomei un Komisijai ziņojumu par šīs iedaļas piemērošanu.

30. pants

Galvenā pārrauga uzdevumi

1. Galvenais pārraugs novērtē, vai katrai kritiski svarīgajai trešai personai, kas sniedz IKT pakalpojumus, ir ieviesti visaptveroši, stabili un efektīvi noteikumi, procedūras, mehānismi un kārtība, lai pārvaldītu IKT riskus, ko tā var radīt finanšu vienībām.

2. Šā panta 1. punktā minētais novērtējums ietver:

(a) IKT prasības, lai jo īpaši nodrošinātu to pakalpojumu drošību, pieejamību, nepārtrauktību, mērogojamību un kvalitāti, kurus kritiski svarīgā trešā persona, kas sniedz IKT pakalpojumus, sniedz finanšu vienībām, kā arī spēju nepārtraukti uzturēt augstus drošības, konfidencialitātes un integritātes standartus;

(b) fizisko drošību, kas palīdz nodrošināt IKT drošību, ieskaitot telpu, objektu, datu centru drošību;

(c) riska pārvaldības procesus, ieskaitot IKT riska pārvaldības rīcībpolitiku, IKT darbības nepārtrauktības un IKT negadījuma seku novēršanas plānus;

(d) pārvaldības kārtību, tostarp organizatorisku struktūru ar skaidriem, pārredzamiem un konsekventiem atbildības un pārskatatbildības noteikumiem, kas ļauj veikt efektīvu IKT riska pārvaldību;

(e) ar IKT saistītu incidentu apzināšanu, uzraudzību un tūlītēju paziņošanu finanšu vienībām, šo incidentu, jo īpaši kiberuzbrukumu, pārvaldību un atrisināšanu;

(f) datu pārnesamības, lietojumprogrammu pārnesamības un sadarbspējas mehānismus, kas finanšu vienībām nodrošina izbeigšanas tiesību efektīvu īstenošanu;

(g) IKT sistēmu, infrastruktūras un kontroles testēšanu;

(h) IKT revīzijas;

(i) tādu attiecīgu valsts un starptautisko standartu izmantošanu, ko piemēro IKT pakalpojumu sniegšanai finanšu vienībām.

3. Balstoties uz 1. punktā minēto novērtējumu, galvenais pārraugs pieņem skaidru, detalizētu un pamatotu individuālās pārraudzības plānu attiecībā uz katru kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus. Šo plānu katru gadu paziņo kritiski svarīgajai trešai personai, kas sniedz IKT pakalpojumus.

4. Tiklīdz 3. punktā minētie gada pārraudzības plāni ir saskaņoti un paziņoti kritiski svarīgajām trešām personām, kas sniedz IKT pakalpojumus, kompetentās iestādes

attiecībā uz kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, var veikt pasākumus tikai ar galvenā pārrauga piekrišanu.

31. pants

Galvenā pārrauga pilnvaras

1. Pildot šajā iedaļā paredzētos pienākumus, galvenajam pārraugam ir šādas pilnvaras:

   (a) pieprasīt visu attiecīgo informāciju un dokumentus saskaņā ar 32. pantu;

   (b) veikt vispārēju izmeklēšanu un pārbaudes saskaņā ar 33. un 34. pantu;

   (c) pieprasīt ziņojumus pēc pārraudzības darbību pabeigšanas, kuros ir norādītas kritiski svarīgo trešo personu, kas sniedz IKT pakalpojumus, veiktās darbības vai īstenotie novēršanas pasākumi saistībā ar šā punkta d) apakšpunktā minētajiem ieteikumiem;

   (d) sniegt ieteikumus attiecībā uz 30. panta 2. punktā minētajām jomām, jo īpaši saistībā ar šādiem jautājumiem:

      i) konkrētu IKT drošības un kvalitātes prasību vai procesu izmantošanu, jo īpaši saistībā ar ielāpu, atjauninājumu, šifrēšanas un citu drošības pasākumu ieviešanu, kurus galvenais pārraugs uzskata par nozīmīgiem finanšu vienībām sniegto pakalpojumu IKT drošības nodrošināšanai;

      ii) noteikumu un nosacījumu izmantošanu, ieskaitot to tehnisko īstenošanu, saskaņā ar kuriem finanšu vienībām IKT pakalpojumus sniedz kritiski svarīgas trešās personas un kurus galvenais pārraugs uzskata par nozīmīgiem saistībā ar viena kļūdaina ķēdes punkta rašanās novēršanu vai tā pastiprināšanu, vai IKT koncentrācijas riska gadījumā — iespējamās sistēmiskās ietekmes uz Savienības finanšu nozari mazināšanu;

      iii) pēc saskaņā ar 32. un 33. pantu veiktas pārbaudes attiecībā uz apakšuzņēmuma līgumiem, tostarp apakšuzņēmuma tālāku deleģēšanu, ko kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, plāno darīt ar citām trešām personām, kas sniedz IKT pakalpojumus, vai ar trešā valstī reģistrētiem IKT apakšuzņēmējiem, jebkuriem plānotiem apakšuzņēmuma līgumiem, tostarp apakšuzņēmuma tālāku deleģēšanu, ja galvenais pārraugs uzskata, ka tālāka apakšuzņēmuma slēgšana var radīt risku finanšu vienības pakalpojumu sniegšanai vai finanšu stabilitātes risku;

      iv) atteikšanos noslēgt tālākus apakšuzņēmuma līgumus, ja ir spēkā šādi kumulatīvi nosacījumi:

         – paredzētais apakšuzņēmējs ir trešā valstī reģistrēta trešā persona, kas sniedz IKT pakalpojumus, vai IKT apakšuzņēmējs;

         – apakšuzņēmuma līguma slēgšana attiecas uz kritiski svarīgu vai svarīgu finanšu vienības funkciju.

2. Pirms 1. punktā minēto pilnvaru izmantošanas galvenais pārraugs apspriežas ar Pārraudzības forumu.

3. Kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, labticīgi sadarbojas ar galveno pārraugu un palīdz galvenajam pārraugam pildīt tā uzdevumus.

4. Galvenais pārraugs var piemērot periodisku sodu maksājumu, lai piespiestu kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, pildīt 1. punkta a), b) un c) apakšpunkta prasības.

5. Šā panta 4. punktā minēto periodisko soda maksājumu piemēro katru dienu, līdz tiek panākta atbilstības prasību ievērošana, bet ne ilgāk kā sešus mēnešus pēc tam, kad par to paziņots kritiski svarīgai trešai personai, kas sniedz IKT pakalpojumus.

6. Periodiskā soda maksājuma summa, rēķinot no lēmumā par periodiska soda maksājuma piemērošanu paredzētā datuma, ir 1 % no kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, dienas vidējā apgrozījuma pasaulē iepriekšējā finanšu gadā.

7. Soda maksājums ir administratīvs un izpildāms piespiedu kārtā. Izpildi reglamentē tās valsts spēkā esošās civilprocesa normas, kurā veic pārbaudes un notiek piekļuve. Attiecīgās dalībvalsts tiesām ir piekritīgas ar izpildes procesa pārkāpumiem saistītās sūdzības. Soda maksājumu summas ieskaita Eiropas Savienības vispārējā budžetā.

8. EUI publisko informāciju par visiem periodiskiem soda maksājumiem, kas piemēroti, ja vien šādas informācijas publiskošana būtiski nekaitē finanšu tirgiem vai nerada nesamērīgu kaitējumu iesaistītajām personām.

9. Galvenais pārraugs pirms periodiska soda maksājuma piemērošanas saskaņā ar 4. punktu nodrošina procesā iesaistītā kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, pārstāvjiem tiesības tikt uzklausītiem attiecībā uz konstatējumiem, kā arī pamato savus lēmumus tikai ar konstatējumiem, par kuriem procesā iesaistītajām kritiski svarīgajām trešām personām, kas sniedz IKT pakalpojumus, ir bijis iespējams izteikties. Lietas izskatīšanā pilnībā ievēro procesā iesaistīto personu tiesības uz aizstāvību. Šīs personas ir tiesīgas piekļūt lietas materiāliem, ievērojot citu personu likumīgās intereses attiecībā uz viņu komercnoslēpumu aizsardzību. Tiesības piekļūt lietas materiāliem neattiecas uz konfidenciālu informāciju vai galvenā pārrauga iekšējiem darba sagatavošanas dokumentiem.

32. pants

Informācijas pieprasījums

1. Galvenais pārraugs ar vienkāršu pieprasījumu vai lēmumu var noteikt, ka kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, ir jāsniedz visa informācija, kas galvenajam pārraugam ir nepieciešama, lai pildītu šajā regulā noteiktos pienākumus, ieskaitot visus attiecīgos darījumdarbības vai darbības dokumentus, līgumus, rīcībpolitikas dokumentus, IKT drošības revīzijas ziņojumus, ar IKT saistītu incidentu ziņojumus, kā arī jebkuru informāciju, kas ir saistīta ar personām, kam kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, ir nodevusi ārpakalpojumā darbības funkcijas vai darbības.

2. Sūtot vienkāršu pieprasījumu sniegt informāciju saskaņā ar 1. punktu, galvenais pārraugs:

   (a) atsaucas uz šo pantu kā pieprasījuma juridisko pamatu;

   (b) norāda pieprasījuma mērķi;

   (c) norāda, kāda informācija ir vajadzīga;

   (d) nosaka termiņu, līdz kuram informācija ir jāsniedz;

(e) informē kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus un no kuras tiek pieprasīta informāciju, pārstāvi, ka tā var nesniegt šo informāciju, bet, ja tā atbildi sniedz brīvprātīgi, sniegtā informācija nedrīkst būt nepatiesa un maldinoša.

3. Pieprasot sniegt informāciju saskaņā ar 1. punktu, galvenais pārraugs:

(a) atsaucas uz šo pantu kā pieprasījuma juridisko pamatu;

(b) norāda pieprasījuma mērķi;

(c) norāda, kāda informācija ir vajadzīga;

(d) nosaka termiņu, līdz kuram informācija ir jāsniedz;

(e) norāda 31. panta 4. punktā paredzēto periodisko soda maksājumu, ja pieprasītā informācija nav sniegta pilnā apmērā;

(f) norāda uz tiesībām šo lēmumu apstrīdēt EUI Apelācijas padomē un uz iespēju to pārskatīt Eiropas Savienības Tiesā ("Tiesa") attiecīgi saskaņā ar Regulas (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010 60. un 61. pantu.

4. Kritiski svarīgo trešo personu, kas sniedz IKT pakalpojumus, pārstāvji sniedz pieprasīto informāciju. Juristi, kas ir attiecīgi pilnvaroti rīkoties, var sniegt informāciju savu klientu vārdā. Kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, ir pilnībā atbildīga, ja sniegtā informācija ir nepilnīga, nepareiza vai maldinoša.

5. Galvenais pārraugs nekavējoties nosūta lēmuma kopiju, lai sniegtu informāciju to finanšu vienību kompetentajām iestādēm, kuras izmanto IKT pakalpojumus, ko sniedz kritiski svarīgās trešās personas.

33. pants
Vispārēja izmeklēšana

1. Lai veiktu savus pienākumus saskaņā ar šo regulu, galvenais pārraugs, kam palīdz 34. panta 1. punktā minētā pārbaudes grupa, var veikt trešo personu, kas sniedz IKT pakalpojumus, vajadzīgo izmeklēšanu.

2. Galvenais pārraugs ir pilnvarots:

(a) pārbaudīt uzskaites dokumentus, datus, procedūras un pārējos materiālus, kas saistīti ar tā uzdevumu izpildi, neatkarīgi no tā, kādā veidā šī informācija tiek glabāta;

(b) iegūt šādu uzskaites dokumentu, datu, procedūru un citu materiālu apstiprinātas kopijas vai izrakstus;

(c) uzaicināt trešās personas, kas sniedz IKT pakalpojumus, pārstāvjus sniegt mutiskus vai rakstiskus paskaidrojumus par faktiem vai dokumentiem, kas attiecas uz izmeklēšanas priekšmetu un mērķi, un fiksēt atbildes;

(d) iztaujāt jebkuru citu fizisku vai juridisku personu, kas piekrīt iztaujāšanai, lai iegūtu informāciju, kas saistīta ar izmeklēšanas priekšmetu;

(e) pieprasīt telefona sarunu izdrukas vai datplūsmas pārskatus.

3. Amatpersonas un citas personas, ko galvenais pārraugs pilnvarojis veikt 1. punktā minēto izmeklēšanu, īsteno savas pilnvaras, uzrādot rakstisku atļauju, kurā norādīts izmeklēšanas priekšmets un mērķis.

   Minētajā atļaujā norāda arī 31. panta 4. punktā paredzētos periodiskos soda maksājumus, ja pieprasīto ierakstu, datu, procedūru vai citu materiālu sagatavošana vai atbilžu sniegšana uz trešās personas, kas sniedz IKT pakalpojumus, pārstāvjiem uzdotajiem jautājumiem nenotiek vai ir nepilnīga.

4. Trešo personu, kas sniedz IKT pakalpojumus, pārstāvjiem ir jāpakļaujas izmeklēšanai, pamatojoties uz galvenā pārrauga lēmumu. Lēmumā nosaka izmeklēšanas priekšmetu un mērķi, periodiskos soda maksājumus, kas paredzēti 31. panta 4. punktā, tiesiskās aizsardzības līdzekļus, kuri pieejami saskaņā ar Regulu (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010, un tiesības vērsties Tiesā, lai šo lēmumu pārskatītu.

5. Galvenie pārraugi laicīgi pirms izmeklēšanas informē to finanšu vienību kompetentās iestādes, kas izmanto IKT pakalpojumus, ko sniedz šīs trešās personas, par izmeklēšanu un atļauju saņēmušo personu identitāti.

34. pants

Pārbaudes uz vietas

1. Lai veiktu savus pienākumus saskaņā ar šo regulu, galvenais pārraugs, kam palīdz 35. panta 1. punktā minētās pārbaudes grupas, var ieiet un veikt visas vajadzīgās pārbaudes uz vietas visās trešo personu, kas sniedz IKT pakalpojumus, uzņēmuma telpās, zemes gabalos vai īpašumos, piemēram, galvenajos birojos, operāciju centros, rezerves telpās, kā arī veikt pārbaudes bezsaistē.

2. Amatpersonas un citas personas, kuras galvenais pārraugs ir pilnvarojis veikt pārbaudi uz vietas, var iekļūt jebkādās šādas uzņēmējdarbības telpās, zemesgabalos vai īpašumos, un tām ir visas pilnvaras aizzīmogot jebkādas uzņēmuma telpas un grāmatas vai ierakstus par pārbaudes laiku un tādā apjomā, kādā tas nepieciešams pārbaudei.

   Tās īsteno savas pilnvaras, uzrādot rakstisku atļauju, kurā norādīts pārbaudes priekšmets un mērķis, kā arī 31. panta 4. punktā paredzētie periodiskie soda maksājumi gadījumam, ja attiecīgo trešo personu, kas sniedz IKT pakalpojumus, pārstāvji nepakļaujas pārbaudei.

3. Galvenie pārraugi laikus pirms pārbaudes informē to finanšu vienību kompetentās iestādes, kas izmanto IKT pakalpojumus, ko sniedz šī trešā persona.

4. Pārbaudes aptver visu attiecīgo IKT sistēmu, tīklu, ierīču, informācijas un datu klāstu, ko izmanto pakalpojumu sniegšanai finanšu vienībām vai kas sekmē šādu pakalpojumu sniegšanu.

5. Pirms plānotās vizītes uz vietas galvenie pārraugi saprātīgā termiņā par to paziņo kritiski svarīgajām trešām personām, kas sniedz IKT pakalpojumus, ja vien šāds paziņojums nav iespējams ārkārtas vai krīzes situācijas dēļ vai ja tas radītu situāciju, kad pārbaude vai revīzija vairs nebūtu efektīva.

6. Kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, pakļaujas pārbaudei uz vietas, ko uzdots veikt ar galvenā pārrauga lēmumu. Šajā lēmumā norāda pārbaudes priekšmetu un mērķi, nosaka dienu, kurā tā sāksies, un norāda periodiskos soda maksājumus, kas paredzēti 31. panta 4. punktā, tiesiskās aizsardzības līdzekļus, kas

pieejami saskaņā ar Regulu (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010, kā arī tiesības vērsties Tiesā, lai šo lēmumu pārskatītu.

7. Ja galvenā pārrauga pilnvarotās amatpersonas un citas personas konstatē, ka kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, iebilst pret pārbaudi, kas noteikta saskaņā ar šo pantu, galvenais pārraugs informē kritiski svarīgo IKT pakalpojumu sniedzēju par šāda iebilduma sekām, tostarp par iespēju attiecīgo finanšu vienību kompetentajām iestādēm izbeigt ar šo kritiski svarīgo trešo personu, kas sniedz IKT pakalpojumus, noslēgtās līgumiskās vienošanās.

35. pants

Pastāvīgā pārraudzība

1. Veicot vispārēju izmeklēšanu vai pārbaudes uz vietas, galvenajam pārraugam palīdz katrai kritiski svarīgajai trešai personai, kas sniedz IKT pakalpojumus, izveidota pārbaudes grupa.

2. Šā panta 1. punktā minēto kopīgo pārbaudes grupu veido galvenā pārrauga un attiecīgo kompetento iestāžu, kas uzrauga finanšu vienības, kurām IKT pakalpojumus sniedz kritiski svarīga trešā persona, darbinieki, kuri pievienojas pārraudzības darbību sagatavošanai un izpildei, nepārsniedzot 10 locekļu skaitu. Visiem kopīgās pārbaudes dalībniekiem ir zināšanas IKT un operacionālā riska jomā. Kopīgā pārbaudes grupa strādā iecelta EUI darbinieka (“galvenā pārrauga koordinators”) vadībā.

3. EUI ar Apvienotās komitejas starpniecību izstrādā kopēju regulatīvo tehnisko standartu projektus, lai sīkāk precizētu to kopīgās pārbaudes grupas locekļu iecelšanu, kas nāk no attiecīgajām kompetentajām iestādēm, kā arī pārbaudes grupas uzdevumus un darba kārtību. EUI iesniedz Komisijai minēto regulatīvo tehnisko standartu projektus līdz [*OV: ievietot datumu, kas ir vienu gadu pēc spēkā stāšanās dienas*].

   Komisijai tiek deleģētas pilnvaras pieņemt šā panta pirmajā daļā minētos regulatīvos tehniskos standartus attiecīgi saskaņā ar 10.–14. pantu Regulā (ES) Nr. 1093/2010, Regulā (ES) Nr. 1095/2010 un Regulā (ES) Nr. 1094/2010.

4. Trīs mēnešu laikā pēc tam, kad pabeigta izmeklēšana vai pārbaude uz vietas, galvenais pārraugs, apspriežoties ar Pārraudzības forumu, pieņem ieteikumus, ko galvenais pārraugs saskaņā ar 31. pantā minētajām pilnvarām adresē kritiski svarīgajai trešai personai, kas sniedz IKT pakalpojumus.

5. Šā panta 4. punktā minētos ieteikumus nekavējoties paziņo kritiski svarīgajai trešai personai, kas sniedz IKT pakalpojumus, un to finanšu vienību kompetentajām iestādēm, kurām tas sniedz pakalpojumus.

   Lai izpildītu pārraudzības darbības, galvenie pāraugi var ņemt vērā visus attiecīgos trešās personas izsniegtos sertifikātus un trešās personas, kas sniedz IKT pakalpojumus, iekšējās vai ārējās revīzijas ziņojumus, ko darījusi pieejamus kritiski svarīgā trešā persona, kas sniedz IKT pakalpojumus.

36. pants

Saskaņoti nosacījumi, kas ļauj veikt pārraudzību

1. EUI ar Apvienotās komitejas starpniecību izstrādā regulatīvo tehnisko standartu projektus, lai noteiktu:

(a) informāciju, ko pieteikumā par 28. panta 8. punktā paredzēto brīvprātīgo iestāšanos sniedz kritiski svarīgā trešā persona, kas sniedz IKT pakalpojumus;

(b) ziņojumu saturu un formātu, ko var pieprasīt 31. panta 1. punkta c) apakšpunkta vajadzībām;

(c) informācijas sniegšanu, tostarp struktūru, formātus un metodes, kas kritiski svarīgajai trešai personai, kas sniedz IKT pakalpojumus, jāizmanto, lai iesniegtu, atklātu vai ziņotu informāciju saskaņā ar 31. panta 1. punktu;

(d) detalizētu informāciju par kompetento iestāžu veikto novērtējumu attiecībā uz pasākumiem, ko veic kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, pamatojoties uz galveno pārraugu ieteikumiem saskaņā ar 37. panta 2. punktu.

2. EUI iesniedz Komisijai minēto regulatīvo tehnisko standartu projektus līdz [*PB: ievietot datumu, kas ir vienu gadu pēc spēkā stāšanās dienas*].

Komisijai tiek deleģētas pilnvaras papildināt šo regulu, pieņemot pirmajā daļā minētos regulatīvos tehniskos standartus attiecīgi saskaņā ar 10.–14. pantu Regulā (ES) Nr. 1093/2010, Regulā (ES) Nr. 1095/2010 un Regulā (ES) Nr. 1094/2010.

37. pants

Kompetento iestāžu turpmākā rīcība

1. Attiecīgā termiņā, kas ir 30 kalendārās dienas pēc galveno pārraugu sniegto ieteikumu saņemšanas saskaņā ar 31. panta 1. punkta d) apakšpunktu, kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, paziņo galvenajam pārraugam par to, vai viņi plāno ievērot minētos ieteikumus. Galvenie pārraugi šo informāciju nekavējoties pārsūta kompetentajām iestādēm.

2. Kompetentās iestādes uzrauga, vai finanšu vienības ņem vērā riskus, kas identificēti ieteikumos, kurus saskaņā ar 31. panta 1. punkta d) apakšpunktu kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, adresējis galvenais pārraugs.

3. Kompetentās iestādes saskaņā ar 44. pantu var noteikt finanšu vienībām pienākumu īslaicīgi pilnībā vai daļēji apturēt tāda IKT pakalpojuma izmantošanu vai izvietošanu, ko sniedz kritiski svarīga trešā persona, kamēr nav novērsti kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, adresētajos ieteikumos identificētie riski. Ja nepieciešams, tās var noteikt, ka finanšu vienībām ir pilnībā vai daļēji jāizbeidz attiecīgās līgumiskas vienošanās, kas ir noslēgtas ar kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus.

4. Pieņemot 3. punktā minētos lēmumus, kompetentās iestādes ņem vērā kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, nenovērstā riska veidu un tā lielumu, kā arī neatbilstības smagumu saskaņā ar šādiem kritērijiem:

(a) neatbilstības smagumu un ilgumu;

(b) vai neatbilstība ir atklājusi būtiskus trūkumus kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, procedūrās, vadības sistēmā, riska pārvaldībā un iekšējā kontrolē;

(c) vai neatbilstība ir veicinājusi vai izraisījusi finanšu noziegumu vai kā citādi ir ar to saistīta;

(d) vai neatbilstība ir notikusi tīši vai nolaidības dēļ.

5. Kompetentās iestādes regulāri informē galvenos pārraugus par pieejām un pasākumiem, ko tās veikušas, pildot finanšu vienību uzraudzības uzdevumus, kā arī par līgumiskajiem pasākumiem, ko tās veikušas, ja kritiski svarīgā trešā persona, kas sniedz IKT pakalpojumus, nav daļēji vai pilnībā apstiprinājusi galvenais pārrauga tai adresētos ieteikumus.

38. pants
Pārraudzības maksas

1. EUI no kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, iekasē maksas, kas pilnībā sedz EUI obligātos izdevumus par pārraudzības uzdevumiem, ko veic saskaņā ar šo regulu, ieskaitot kompetento iestāžu, kas piedalās pārraudzības darbībās saskaņā ar 35. pantu, veiktā darba izmaksu atlīdzināšanu.

   Kritiski svarīgai trešai personai, kas sniedz IKT pakalpojumus, piemērotās maksas sedz visas administratīvās izmaksas un ir proporcionālas tā apgrozījumam.

2. Komisija ir pilnvarota pieņemt deleģēto aktu saskaņā ar 50. pantu, lai papildinātu šo regulu, nosakot maksas apmēru un tās samaksas veidu.

39. pants
Starptautiskā sadarbība

1. EBI, EVTI un EAAPI attiecīgi saskaņā ar Regulas (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010 33. pantu var noslēgt administratīvas vienošanās ar trešo valstu regulatīvajām un uzraudzības iestādēm, lai veicinātu starptautisku sadarbību attiecībā uz IKT risku, kas saistīts ar trešo personu, dažādās finanšu nozarēs, jo īpaši izstrādājot IKT riska pārvaldības labākās prakses un kontroles, ietekmes mazināšanas pasākumu un incidentu atbilžu pārskatīšanas labāko praksi.

2. EUI ar Apvienotās komitejas starpniecību ik pēc pieciem gadiem iesniedz Eiropas Parlamentam, Padomei un Komisijai kopīgu konfidenciālu ziņojumu, kurā apkopoti secinājumi par attiecīgajām diskusijām ar 1. punktā minētajām trešo valstu iestādēm, veltot uzmanību ar trešo personu saistītā IKT riska attīstībai un ietekmei uz finanšu stabilitāti, tirgus integritāti, ieguldītāju aizsardzību vai vienotā tirgus darbību.

VI NODAĻA

INFORMĀCIJAS APMAIŅAS KĀRTĪBA

40. pants
Kiberdraudu informācijas un izlūkdatu informācijas apmaiņas kārtība

1. Finanšu vienības var savstarpēji apmainīties ar informāciju par kiberdraudiem un izlūkdatiem, tajā skaitā pazīmēm, kas liecina par kompromitēšanu, taktiku, paņēmieniem un procedūrām, kiberdraudu trauksmes signāliem un konfigurēšanas rīkiem, ciktāl šāda informācijas un izlūkdatu koplietošana:

   (a) ir ar mērķi uzlabot finanšu vienību digitālās darbības noturību, jo īpaši palielinot informētību attiecībā uz kiberdraudiem, ierobežojot vai traucējot kiberdraudu izplatīšanos, atbalstot finanšu vienību aizsardzības spējas,

apdraudējuma atklāšanas metodes, seku mazināšanas stratēģijas vai reaģēšanas un seku novēršanas posmus;

(b) notiek uzticamās finanšu vienību kopienās;

(c) tiek īstenota, izmantojot informācijas apmaiņas pasākumus, kas aizsargā koplietotās informācijas iespējami sensitīvo raksturu, un ko reglamentē rīcības noteikumi, kuros pilnībā ievērota uzņēmējdarbības konfidencialitāte, personas datu aizsardzība[48] un nostādnes par konkurences politiku[49].

2. Šā panta 1. punkta c) apakšpunkta vajadzībām informācijas apmaiņas kārtība nosaka dalības nosacījumus un vajadzības gadījumā sīkāk nosaka valsts iestāžu iesaisti un statusu, kādā tās var būt saistītas ar informācijas apmaiņas kārtību, kā arī par darbības elementiem, tostarp specializētu IT platformu izmantošanu.

3. Finanšu vienības paziņo kompetentajām iestādēm par savu dalību 1. punktā minētajos informācijas apmaiņas pasākumos pēc to dalības atzīšanas vai attiecīgā gadījumā — dalības izbeigšanas, kad tā stājusies spēkā.

VII NODAĻA

KOMPETENTĀS IESTĀDES

41. pants

Kompetentās iestādes

Neskarot šīs regulas V nodaļas II iedaļā minētos noteikumus par kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, pārraudzības sistēmu, šajā regulā noteikto saistību izpildi saskaņā ar pilnvarām, kas piešķirtas ar attiecīgiem tiesību aktiem, nodrošina šādas kompetentās iestādes:

(a) kredītiestādēm — kompetentā iestāde, kas norīkota saskaņā ar Direktīvas 2013/36/ES 4. pantu, neskarot īpašos uzdevumus, kas ECB uzticēti ar Regulu (ES) Nr. 1024/2013;

(b) maksājumu pakalpojumu sniedzējiem — kompetentā iestāde, kas norīkota saskaņā ar Direktīvas (ES) 2015/2366 22. pantu;

(c) elektronisko maksājumu iestādēm — kompetentā iestāde, kas norīkota saskaņā ar Direktīvas 2009/110/EK 37. pantu;

(d) ieguldījumu brokeru sabiedrībām — kompetentā iestāde, kas norīkota saskaņā ar Direktīvas (ES) 2019/2034 4. pantu;

(e) kriptoaktīvu pakalpojumu sniedzējiem, kriptoaktīvu emitentiem, aktīviem piesaistītu tokenu emitentiem un nozīmīgu aktīviem piesaistītu tokenu emitentiem — kompetentā iestāde, kas norīkota saskaņā ar [*Regulas (ES) Nr. 20xx, KAT regula*] 3. panta 1. punkta ee) apakšpunkta pirmo ievilkumu;

---

48 Saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

49 Komisijas paziņojums "Pamatnostādnes par Līguma par Eiropas Savienības darbību 101. panta piemērojamību horizontālās sadarbības nolīgumiem", 2011/C 11/01.

(f) centrālajiem vērtspapīru depozitārijiem — kompetentā iestāde, kas norīkota saskaņā ar Regulas (ES) Nr. 909/2014 11. pantu;

(g) centrālajiem darījumu partneriem — kompetentā iestāde, kas norīkota saskaņā ar Regulas (ES) Nr. 648/2012 22. pantu;

(h) tirdzniecības vietām un datu ziņošanas pakalpojumu sniedzējiem — kompetentā iestāde, kas norīkota saskaņā ar Direktīvas 2014/65/ES 67. pantu;

(i) darījumu reģistriem — kompetentās iestādes, kas norīkotas saskaņā ar Regulas (ES) Nr. 648/2012 55. pantu;

(j) alternatīvo ieguldījumu fondu pārvaldniekiem — kompetentā iestāde, kas norīkota saskaņā ar Direktīvas 2011/61/EK 44. pantu;

(k) pārvaldības sabiedrībām — kompetentā iestāde, kas norīkota saskaņā ar Direktīvas 2009/65/EK 97. pantu;

(l) apdrošināšanas sabiedrībām un pārapdrošināšanas sabiedrībām — kompetentā iestāde, kas norīkota saskaņā ar Direktīvas 2009/138/EK 30. pantu;

(m) apdrošināšanas starpniekiem, pārapdrošināšanas starpniekiem un apdrošināšanas papildpakalpojuma starpniekiem — kompetentā iestāde, kas norīkota saskaņā ar Direktīvas (ES) 2016/97 12. pantu;

(n) arodpensiju iestādēm — kompetentā iestāde, kas norīkota saskaņā ar Direktīvas 2016/2341/EK 47. pantu;

(o) kredītreitingu aģentūrām — kompetentā iestāde, kas norīkota saskaņā ar Direktīvas (ES) 1060/2009 21. pantu;

(p) obligātajiem revidentiem un revīzijas uzņēmumiem — kompetentā iestāde, kas norīkota saskaņā ar Direktīvas 2006/43/EK 32. pantu un 3. panta 3. punktu;

(q) kritiski svarīgu etalonu administratoriem — kompetentā iestāde, kas norīkota saskaņā ar *Regulas xx/202x* 40. un 41. pantu;

(r) kolektīvās finansēšanas pakalpojumu sniedzējiem — kompetentā iestāde, kas norīkota saskaņā ar *Regulas xx/202x x. pantu*;

(s) vērtspapīrošanas repozitorijiem — kompetentā iestāde, kas norīkota saskaņā ar Regulas (ES) Nr. 2017/2402 10. pantu un 14. panta 1. punktu.

42. pants

Sadarbība ar struktūrām un iestādēm, kas izveidotas ar Direktīvu (ES) 2016/1148

1. Lai sekmētu sadarbību un ļautu veikt uzraudzības apmaiņu starp kompetentajām iestādēm, kas ieceltas ar šo regulu, un saskaņā ar Direktīvas (ES) 2016/1148 11. pantu izveidoto sadarbības grupu, EUI un kompetentās iestādes var pieprasīt, lai tās pieaicina sadarbības grupas darbā.

2. Kompetentās iestādes vajadzības gadījumā var konsultēties ar vienoto kontaktpunktu un valstu datordrošības incidentu reaģēšanas vienībām, kas minētas attiecīgi Direktīvas (ES) 2016/1148 8. un 9. pantā.

43. pants

Finanšu starpnozaru mācības, saziņa un sadarbība

1. EUI ar Apvienotās komitejas starpniecību un sadarbībā ar kompetentajām iestādēm, ECB un ESRK var izveidot mehānismus, kas ļauj apmainīties ar efektīvu praksi starp finanšu nozarēm, lai uzlabotu informētību par situāciju un noteiktu starpnozaru kopīgo kiberneaizskaramību un riskus.

   Tās var izstrādāt krīzes pārvarēšanas un ārkārtas situāciju pasākumus, kuros ietilpst kiberuzbrukuma scenāriji, lai attīstītu saziņas kanālus un pakāpeniski nodrošinātu efektīvu ES līmeņa koordinētu reakciju, ja būtisks pārrobežu IKT incidents vai ar to saistīts apdraudējums radītu sistēmisku ietekmi uz Savienības finanšu nozari kopumā.

   Šajās mācībās vajadzības gadījumā var arī pārbaudīt finanšu nozares atkarību no citām ekonomikas nozarēm.

2. Kompetentās iestādes, EBI, EVTI vai EAAPI un ECB cieši sadarbojas savā starpā un apmainās ar informāciju, lai veiktu savus pienākumus saskaņā ar 42.–48. pantu. Kompetentās iestādes cieši koordinē uzraudzību, lai apzinātu un novērstu šīs regulas pārkāpumus, izstrādātu un sekmētu labāko praksi, veicinātu sadarbību, stiprinātu interpretācijas saskaņotību un nodrošinātu vairākjurisdikciju novērtējumus jebkādu domstarpību gadījumā.

44. pants

Administratīvi sodi un korektīvi pasākumi

1. Kompetentajām iestādēm ir visas uzraudzības, izmeklēšanas un sankciju pilnvaras, kas vajadzīgas, lai izpildītu pienākumus saskaņā ar šo regulu.

2. Šā panta 1. punktā minētās pilnvaras ietver vismaz šādas pilnvaras:

   (a) piekļūt jebkuram dokumentam vai datiem jebkādā formātā, kurus kompetentās iestādes uzskata par nozīmīgiem tās uzraudzības pienākumu veikšanā, un saņemt to kopiju vai nokopēt tos;

   (b) veikt pārbaudes uz vietas vai izmeklēšanu;

   (c) pieprasīt koriģējošus un korektīvus pasākumus šīs regulas prasību pārkāpšanas gadījumos.

3. Neskarot dalībvalstu tiesības piemērot krimināl sodus saskaņā ar 46. pantu, dalībvalstis paredz noteikumus, ar ko nosaka attiecīgus administratīvos sodus un korektīvus pasākumus šīs regulas pārkāpumu gadījumos, kā arī nodrošina to efektīvu īstenošanu.

   Šiem sodiem un pasākumiem jābūt iedarbīgiem, samērīgiem un atturošiem.

4. Dalībvalstis piešķir kompetentajām iestādēm pilnvaras par šīs regulas pārkāpumiem piemērot vismaz šādus administratīvos sodus vai korektīvus pasākumus:

   (a) izdot rīkojumu fiziskai vai juridiskai personai pārtraukt attiecīgo rīcību un atturēties no tās atkārtošanas;

   (b) pieprasīt pagaidu vai pastāvīgu jebkuras prakses vai rīcības pārtraukšanu, ko kompetentā iestāde uzskata par pretēju šīs regulas noteikumiem, un novērst minētās prakses vai rīcības atkārtošanos;

(c) pieņemt jebkāda veida pasākumus, tostarp finansiāla rakstura pasākumus, lai nodrošinātu to, ka finanšu vienības turpina ievērot juridiskās prasības;

(d) ciktāl to atļauj valsts tiesību akti, pieprasīt telesakaru operatora rīcībā esošos datu plūsmas ierakstus, ja ir pamatotas aizdomas par šīs regulas pārkāpumu un ja šādi ieraksti var būt noderīgi, izmeklējot šīs regulas pārkāpumus; kā arī

(e) izdot publiskus paziņojumus, tostarp publiskus paziņojumus, kuros norādīta fiziskās vai juridiskās personas identitāte un pārkāpuma būtība.

5. Ja 2. punkta c) apakšpunktā un 4. punktā minētie noteikumi attiecas uz juridiskām personām, dalībvalstis, ievērojot valsts tiesību aktos paredzētos nosacījumus, piešķir kompetentajām iestādēm pilnvaras piemērot administratīvos sodus un korektīvos pasākumus vadības struktūras locekļiem un citām personām, kas saskaņā ar valsts tiesību aktiem ir saucamas pie atbildības par pārkāpumu.

6. Dalībvalstis nodrošina, ka jebkurš lēmums, ar ko uzliek 2. punkta c) apakšpunktā minētos administratīvos sodus vai korektīvos pasākumus, ir pienācīgi pamatots un ka uz to attiecas tiesības to pārsūdzēt.

45. pants

Administratīvo sodu un korektīvo pasākumu piemērošanas pilnvaru īstenošana

1. Kompetentās iestādes pēc vajadzības īsteno pilnvaras uzlikt 44. pantā minētos administratīvos sodus un korektīvos pasākumus saskaņā ar attiecīgās valsts tiesisko regulējumu:

(a) tieši;

(b) sadarbojoties ar citām iestādēm;

(c) uz savu atbildību deleģējot savas pilnvaras citām iestādēm; un

(d) iesniedzot pieteikumu kompetentajām tiesas iestādēm.

2. Kompetentās iestādes, nosakot saskaņā ar 44. pantu uzlikta administratīvā soda vai korektīva pasākuma veidu un apmēru, ņem vērā visus nozīmīgos apstākļus, tostarp to, cik lielā mērā pārkāpums izdarīts tīši vai izriet no neuzmanības, un visus citus atbilstīgos apstākļus, tostarp vajadzības gadījumā:

(a) pārkāpuma būtiskumu, smagumu un ilgumu;

(b) fiziskās vai juridiskās personas, kas ir atbildīga par pārkāpumu, atbildības pakāpi;

(c) atbildīgās fiziskās vai juridiskās personas finansiālo stāvokli;

(d) atbildīgās fiziskās vai juridiskās personas gūtās peļņas vai novērsto zaudējumu nozīmīgumu, ciktāl to var noteikt;

(e) pārkāpuma radītos zaudējumus trešām personām, ja tos var noteikt;

(f) atbildīgās personas sadarbības līmeni ar kompetento iestādi, neskarot vajadzību nodrošināt attiecīgās personas gūto ienākumu vai novērsto zaudējumu atdošanu;

(g) atbildīgās fiziskās vai juridiskās personas iepriekš izdarītos pārkāpumus.

46. pants

Kriminālsodi

1. Dalībvalstis var nolemt neparedzēt noteikumus par administratīviem sodiem vai korektīviem pasākumiem attiecībā uz pārkāpumiem, par kuriem saskaņā ar attiecīgās valsts tiesību aktiem piemēro kriminālsodus.

2. Ja dalībvalstis izvēlējušās noteikt kriminālsodus par šīs regulas pārkāpumiem, tās nodrošina, ka ir ieviesti atbilstoši pasākumi, lai kompetentajām iestādēm attiecīgajā tiesību sistēmā būtu visas nepieciešamās pilnvaras koordinēt sadarbību ar tiesu, prokuratūras un tiesībaizsardzības iestādēm, kas vajadzīgas, lai saņemtu konkrētu informāciju, kas saistīta ar kriminālizmeklēšanu vai procedūrām, kas sāktas attiecībā uz šīs regulas pārkāpumiem, un lai to pašu informāciju sniegtu citām kompetentajām iestādēm un EBI, EVTI vai EAAPI, lai izpildītu pienākumu sadarboties šīs regulas vajadzībām.

47. pants

Ziņošanas pienākums

Dalībvalstis Komisijai, EVTI, EBI un EAAPI dara zināmus normatīvos un administratīvos aktus, ar ko īsteno šo nodaļu, tostarp visus attiecīgos krimināltiesību noteikumus [*OV*: *ievietot datumu, kas ir vienu gadu pēc spēkā stāšanās dienas*]. Dalībvalstis bez liekas kavēšanās informē Komisiju, EVTI, EBI un EAAPI par turpmākiem grozījumiem tajos.

48. pants

Informācijas par administratīvajiem sodiem publicēšana

1. Kompetentās iestādes savā oficiālajā tīmekļa vietnē bez nepamatotas kavēšanās publicē jebkuru lēmumu, ar kuru piemērots administratīvais sods, kas nav pārsūdzams, pēc tam, kad par minēto lēmumu ir paziņots soda adresātam.

2. Publikācijā, kas minēta 1. punktā, ietver informāciju par pārkāpuma veidu un būtību, par pārkāpumu atbildīgo personu identitāti un par piemērotajiem sodiem.

3. Ja kompetentā iestāde pēc katrā gadījumā atsevišķi veikta novērtējuma uzskata, ka identitātes publicēšana juridisku personu gadījumā vai identitātes un personas datu publicēšana fizisko personu gadījumā būtu nesamērīga, apdraudētu finanšu tirgu stabilitāti vai notiekošu kriminālizmeklēšanu vai, ciktāl to var noteikt, radītu nesamērīgu kaitējumu attiecīgajai personai, tā attiecībā uz lēmumu, ar ko uzliek administratīvo sodu, pieņem kādu no šādiem risinājumiem:

   (a) atlikt tā publicēšanu līdz brīdim, kad vairs nepastāv neviens nepublicēšanas iemesls;

   (b) publicēt to anonīmi saskaņā ar valsts tiesību aktiem; vai

   (c) atturēties no publicēšanas, ja a) un b) apakšpunktā izklāstītie risinājumi tiek uzskatīti vai nu par nepietiekamiem, lai garantētu finanšu tirgu stabilitātes apdraudējuma neiestāšanos, vai ja šāda publicēšana nebūtu proporcionāla piemērotā soda maigumam.

4. Gadījumā, ja tiek pieņemts lēmums publicēt administratīvo sodu anonīmi, kā minēts 3. punkta b) apakšpunktā, attiecīgo datu publicēšanu var atlikt.

5. Ja kompetentā iestāde publicē lēmumu, ar kuru uzliek administratīvo sodu, kurš ir pārsūdzēts attiecīgajās tiesu iestādēs, kompetentās iestādes nekavējoties savā oficiālajā tīmekļa vietnē ievieto arī šo informāciju un vēlāk — jebkādu turpmāku saistītu informāciju par šādas pārsūdzības iznākumu. Publicē arī jebkuru tiesas nolēmumu, ar ko atceļ lēmumu par administratīvā soda uzlikšanu.

6. Kompetentā iestāde nodrošina, ka jebkura publikācija, kas minēta 1.–4. punktā, tās oficiālajā tīmekļa vietnē ir pieejama vismaz piecus gadus pēc tās publicēšanas. Jebkuri personas dati, kas iekļauti publikācijā, tiek uzglabāti kompetentās iestādes oficiālajā tīmekļa vietnē tikai uz laikposmu, kas nepieciešams saskaņā ar piemērojamiem datu aizsardzības noteikumiem.

49. pants

Dienesta noslēpums

1. Uz konfidenciālu informāciju, kas saņemta, ar ko veikta apmaiņa vai kas nosūtīta, ievērojot šo regulu, attiecas 2. punktā izklāstītie nosacījumi par dienesta noslēpumu.

2. Dienesta noslēpuma ievērošanas pienākums attiecas uz visām personām, ko nodarbina vai ir nodarbinājušas šajā regulā paredzētās kompetentās iestādes vai kāda cita iestāde vai tirgus uzņēmums, vai fiziska vai juridiska persona, kurai kompetentās iestādes ir deleģējušas savas pilnvaras, tostarp arī to nolīgtiem revidentiem un ekspertiem.

3. Informāciju, uz ko attiecas dienesta noslēpums, nevar atklāt nevienai citai personai vai iestādei citādi, nekā ir paredzēts Savienības vai valsts tiesību noteikumos.

4. Visu informāciju, ar ko kompetentās iestādes apmainās saskaņā ar šo regulu un kas attiecas uz darījumu vai darbības apstākļiem un citiem ekonomiska vai personiska rakstura jautājumiem, uzskata par konfidenciālu, un tai piemēro dienesta noslēpuma prasības, ja vien kompetentā iestāde, sniedzot attiecīgo informāciju, nav atļāvusi to izpaust vai ja šāda izpaušana nav nepieciešama tiesvedībai.

VIII NODAĻA

DELEĢĒTIE AKTI

50. pants

Deleģēšanas īstenošana

1. Pilnvaras pieņemt deleģētos aktus Komisijai piešķir, ievērojot šajā pantā izklāstītos nosacījumus.

2. Pilnvaras pieņemt 28. panta 3. punktā un 38. panta 2. punktā minētos deleģētos aktus Komisijai piešķir uz piecu gadu laikposmu no [PB: ievietot datumu, kas ir piecus gadus pēc šīs regulas spēkā stāšanās dienas].

3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 28. panta 3. punktā un 38. panta 2. punktā minēto pilnvaru deleģēšanu. Ar lēmumu par atsaukšanu izbeidz tajā norādīto pilnvaru deleģēšanu. Lēmums stājas spēkā nākamajā dienā pēc tā

publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī* vai vēlākā dienā, kas tajā norādīta. Tas neskar jau spēkā esošos deleģētos aktus.

4. Pirms deleģētā akta pieņemšanas Komisija apspriežas ar ekspertiem, kurus katra dalībvalsts iecēlusi saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu.

5. Tiklīdz tā pieņem deleģētu aktu, Komisija par to paziņo vienlaikus Eiropas Parlamentam un Padomei.

6. Saskaņā ar 28. panta 3. punktu un 38. panta 2. punktu pieņemts deleģētais akts stājas spēkā tikai tad, ja divos mēnešos no dienas, kad minētais akts paziņots Eiropas Parlamentam un Padomei, ne Eiropas Parlaments, ne Padome nav izteikuši iebildumus vai ja pirms minētā laikposma beigām gan Eiropas Parlaments, gan Padome ir informējuši Komisiju par savu nodomu neizteikt iebildumus. Pēc Eiropas Parlamenta vai Padomes iniciatīvas šo laikposmu pagarina par diviem mēnešiem.

IX NODAĻA

PĀREJAS UN NOBEIGUMA NOTEIKUMI

I IEDAĻA

51. pants

Pārskatīšanas klauzula

Komisija līdz [PB: ievietot datumu, kas ir pieci gadi pēc spēkā stāšanās dienas], vajadzības gadījumā — pēc apspriešanās ar EBI, EVTI, EAAPI un ESRK, veic pārskatīšanu un iesniedz ziņojumu Eiropas Parlamentam un Padomei, vajadzības gadījumā pievienojot tiesību akta priekšlikumu attiecībā uz 28. panta 2. punktā paredzētajiem kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, izraudzīšanās kritērijiem.

II IEDAĻA

GROZĪJUMI

52. pants

Grozījumi Regulā (EK) Nr. 1060/2009

Regulas (EK) Nr. 1060/2009 I pielikuma A iedaļas 4. panta pirmo daļu aizstāj ar šādu:

"Kredītreitingu aģentūrai ir pareizas administratīvas un grāmatvedības procedūras, iekšējie kontroles mehānismi, efektīvas riska novērtēšanas procedūras, kā arī efektīvi kontroles pasākumi un aizsargpasākumi IKT sistēmu pārvaldībai saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2021/xx* [DDN].

* Eiropas Parlamenta un Padomes Regula (ES) 2021/xx [...] (OV L XX, DD.MM.GGGG., X. lpp.).".

53. pants

Grozījumi Regulā (ES) Nr. 648/2012

Regulu (ES) Nr. 648/2012 groza šādi:

(1) regulas 26. pantu groza šādi:

(a) panta 3. punktu aizstāj ar šādu:

"3. CCP uztur un izmanto organizatorisko struktūru, kas nodrošina tā pakalpojumu un darbību veikšanas nepārtrauktību un pareizu funkcionēšanu. Tas izmanto piemērotas un samērīgas sistēmas, resursus un procedūras, ieskaitot IKT sistēmas, ko pārvalda saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2021/xx* [DDN].

* Eiropas Parlamenta un Padomes Regula (ES) Nr. 2021/xx [...] (OV L XX, DD.MM.GGGG., X. lpp.).";

(b) panta 6. punktu svītro;

(2) regulas 34. pantu groza šādi:

(a) panta 1. punktu aizstāj ar šādu:

"1. CCP iedibina, īsteno un uztur piemērotu uzņēmējdarbības nepārtrauktības politiku un negadījuma seku novēršanas plānu, kurā ietver saskaņā ar Regulu (ES) 2021/xx [DDN] izveidotus IKT uzņēmējdarbības nepārtrauktības un negadījuma seku novēršanas plānus, ar mērķi nodrošināt tā funkciju saglabāšanu, darbību laicīgu atjaunošanu un CCP izpildi.";

(b) panta 3. punkta pirmo daļu aizstāj ar šādu:

"Lai nodrošinātu šā panta konsekventu piemērošanu, EVTI pēc apspriešanās ar ECBS dalībniekiem izstrādā regulatīvo tehnisko standartu projektus, kuros nosaka uzņēmējdarbības nepārtrauktības politikas un negadījuma seku novēršanas plāna minimālo saturu un prasības, izņemot IKT darbības nepārtrauktības un negadījuma seku novēršanas plānus.";

(3) regulas 56. panta 3. punkta pirmo daļu aizstāj ar šādu daļu:

"3. Lai nodrošinātu šā panta konsekventu piemērošanu, EVTI izstrādā regulatīvo tehnisko standartu projektus, izņemot attiecībā uz IKT riska pārvaldības prasībām, nosakot 1. punktā minēto sīkāko informāciju par reģistrācijas pieteikumu.";

(4) regulas 79. panta 1. un 2. punktu aizstāj ar šādiem:

"1. Darījumu reģistrs identificē darbības riska cēloņus un mazina tos arī, izstrādājot atbilstošas sistēmas, veicot pārbaudi un izmantojot procedūras, tostarp IKT sistēmas, ko pārvalda saskaņā ar Regulu (ES) Nr. 2021/xx [DDN].

2. Darījumu reģistrs izstrādā, īsteno un uztur atbilstošu uzņēmējdarbības nepārtrauktības politiku un negadījuma seku novēršanas plānu, ieskaitot saskaņā ar Regulu (ES) 2021/xx [DDN] izveidotus IKT uzņēmējdarbības nepārtrauktības un negadījuma seku novēršanas plānus un kura mērķis ir nodrošināt savu funkciju uzturēšanu, laicīgu darbības atsākšanu un darījumu reģistra pienākumu turpmāku izpildi.";

(5) regulas 80. panta 1. punktu svītro.

54. pants

Grozījumi Regulā (ES) Nr. 909/2014

Regulas (ES) Nr. 909/2014 45. pantu groza šādi:

(1) panta 1. punktu aizstāj ar šādu:

"1. CVD identificē iekšējos un ārējos operacionālā riska avotus un pēc iespējas samazina to ietekmi, izmantojot atbilstīgus IKT instrumentus, kontroli un rīcībpolitiku, ko izveido un pārvalda saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2021/xx [DDN], tostarp visām tā uzturētajām vērtspapīru norēķinu sistēmām.

* Eiropas Parlamenta un Padomes Regula (ES) Nr. 2021/xx […](OV L XX, DD.MM.GGGG., X. lpp.).";

(2) panta 2. punktu svītro;

(3) panta 3. un 4. punktu aizstāj ar šādu:

"3. CVD attiecībā uz tā sniegtajiem pakalpojumiem, kā arī attiecībā uz katru tā uzturēto vērtspapīru norēķinu sistēmu izveido, ievieš un uztur pienācīgu darbības nepārtrauktības nodrošināšanas politiku un negadījumu seku novēršanas plānu, ieskaitot saskaņā ar Regulu (ES) 2021/xx [DDN] izveidotu IKT darbības nepārtrauktības nodrošināšanas politiku un negadījuma seku novēršanas plānu, lai nodrošinātu, ka tā pakalpojumi tiek saglabāti un CVD darbība un pienākumu pildīšana tiek savlaicīgi atjaunota gadījumos, kad rodas nozīmīgs darbības traucējumu risks.

4. Šā panta 3. punktā minētais plāns paredz atjaunot visus darījumus un dalībnieku pozīcijas darbības pārtraukšanas brīdī, lai CVD dalībnieki varētu turpināt droši darboties un pabeigt norēķinus plānotajā datumā, tostarp nodrošinot, ka kritiskās IT sistēmas var atjaunot darbības no to pārtraukšanas brīža, kā paredzēts Regulas (ES) 2021/xx [DDN] 11. panta 5. un 7. punktā.";

(4) panta 6. punkta pirmo daļu aizstāj ar šādu:

"CVD identificē, uzrauga un pārvalda riskus, kādus tā darbībai var radīt CVD pārvaldīto vērtspapīru norēķinu sistēmu galvenie dalībnieki, kā arī pakalpojumu un komunālo pakalpojumu sniedzēji un citi CVD vai citas tirgus infrastruktūras. Tas pēc pieprasījuma sniedz kompetentajām un attiecīgajām iestādēm informāciju par visiem šādiem identificētiem riskiem. Tas arī nekavējoties informē kompetento iestādi un attiecīgās iestādes par visiem darbības incidentiem, ko izraisa šādi riski, ja tie nav saistīti ar IKT risku.";

(5) panta 7. punkta pirmo daļu aizstāj ar šādu:

"EVTI ciešā sadarbībā ar ECBS dalībniecēm izstrādā regulatīvu tehnisko standartu projektu, lai noteiktu 1. un 6. punktā minētos operacionālos riskus, izņemot IKT riskus, un metodes šādu risku testēšanai, risināšanai un iespējamai mazināšanai, tostarp 3. un 4. punktā minētās darbības nepārtrauktības nodrošināšanas politikas un negadījumu seku novēršanas plānu, kā arī to novērtēšanas metodes.".

55. pants

Grozījumi Regulā (ES) Nr. 600/2014

Regulu (ES) Nr. 600/2014 groza šādi:

(1) regulas 27.g pantu groza šādi:

(a) panta 4. punktu svītro;

(b) panta 8. punkta c) apakšpunktu aizstāj ar šādu:

(c) "c) konkrētas organizatoriskas prasības, kas izklāstītas 3. un 5. punktā.";

(2) regulas 27.h pantu groza šādi:

(a) panta 5. punktu svītro;

(b) panta 8. punkta e) apakšpunktu aizstāj ar šādu:

"e) konkrētas organizatoriskas prasības, kas izklāstītas 4. punktā.";

(3) regulas 27.i pantu groza šādi:

(a) panta 3. punktu svītro;

(b) panta 5. punkta b) apakšpunktu aizstāj ar šādu:

"b) konkrētas organizatoriskas prasības, kas izklāstītas 2. un 4. punktā.".

56. pants

Stāšanās spēkā un piemērošana

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

To piemēro no [*PB: ievietot datumu, kas ir 12 mēnešus pēc spēkā stāšanās dienas*].

Tomēr 23. un 24. pantu piemēro no [*PB*: *ievietot datumu, kas ir 36 mēnešus pēc šīs regulas spēkā stāšanās dienas*].

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē,

Eiropas Parlamenta vārdā	*Padomes vārdā*
priekšsēdētājs	*priekšsēdētājs*

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

1.1. Priekšlikuma/iniciatīvas nosaukums

1.2. Attiecīgā rīcībpolitikas joma

1.3. Priekšlikuma/iniciatīvas būtība

1.4. Mērķi

1.5. Priekšlikuma/iniciatīvas pamatojums

1.6. Priekšlikuma/iniciatīvas ilgums un finansiālā ietekme

1.7. Paredzētie pārvaldības veidi

2. PĀRVALDĪBAS PASĀKUMI

2.1. Pārraudzības un ziņošanas noteikumi

2.2. Pārvaldības un kontroles sistēma

2.3. Krāpšanas un pārkāpumu novēršanas pasākumi

3. PRIEKŠLIKUMA/INICIATĪVAS APLĒSTĀ FINANSIĀLĀ IETEKME

3.1. Attiecīgās daudzgadu finanšu shēmas izdevumu kategorijas un budžeta izdevumu pozīcijas

3.2. Paredzamā ietekme uz izdevumiem

3.2.1. Kopsavilkums par paredzamo ietekmi uz izdevumiem

3.2.2. Paredzamā ietekme uz apropriācijām

3.2.3. Paredzamā ietekme uz cilvēkresursiem

3.2.4. Saderība ar pašreizējo daudzgadu finanšu shēmu

3.2.5. Trešo personu iemaksas

3.3. Aplēstā ietekme uz ieņēmumiem

Pielikums

Vispārējie pieņēmumi

Pārraudzības pilnvaras

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS — "AĢENTŪRAS"

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

1.1. Priekšlikuma/iniciatīvas nosaukums

Priekšlikums Eiropas Parlamenta un Padomes regulai par finanšu nozares digitālās darbības noturību.

1.2. Attiecīgā rīcībpolitikas joma

Politikas joma: Finanšu stabilitāte, finanšu pakalpojumi un kapitāla tirgu savienība

Uzdevums: digitālās darbības noturība

1.3. Priekšlikums attiecas uz

☑ **jaunu darbību**

☐ **jaunu darbību, pamatojoties uz izmēģinājuma projektu / sagatavošanas darbību**[50]

☐ **esošas darbības pagarināšanu**

☐ **vienas vai vairāku darbību apvienošanu ar citu/jaunu darbību**

1.4. Mērķi

1.4.1. Vispārīgie mērķi

Iniciatīvas vispārīgais mērķis ir stiprināt ES finanšu nozares struktūru digitālās darbības noturību, racionalizējot un uzlabojot esošos noteikumus un ieviešot jaunas prasības jomās, kurās pastāv nepilnības. Ar to tiktu stiprināta arī vienotā noteikumu kopuma digitālā dimensija.

Kopējo mērķi var iedalīt trīs vispārīgajos mērķos: 1) mazināt finanšu satricinājumu un nestabilitātes risku, 2) mazināt administratīvo slogu un palielināt uzraudzības efektivitāti un 3) palielināt patērētāju un ieguldītāju aizsardzību.

1.4.2. Konkrētie mērķi

Priekšlikuma konkrētie mērķi ir šādi:

visaptverošāk novērst informācijas un komunikācijas tehnoloģijas (IKT) riskus un stiprināt finanšu nozares digitālās noturības kopējo līmeni;

racionalizēt ar IKT saistīto incidentu paziņošanu un risināt ziņošanas prasību pārklāšanos;

ļaut finanšu uzraudzības iestādēm piekļūt informācijai par incidentiem, kas saistīti ar IKT;

nodrošināt, ka finanšu vienības, uz kurām attiecas šis priekšlikums, izvērtē savu preventīvo un noturības pasākumu efektivitāti un identificē ar IKT saistītu neaizskaramību;

mazināt vienotā tirgus sadrumstalotību un panākt testēšanas rezultātu pārrobežu pieņemšanu.

[50] Kā paredzēts Finanšu regulas 58. panta 2. punkta a) vai b) apakšpunktā.

Stiprināt līgumiskās garantijas finanšu vienībām, kas izmanto IKT pakalpojumus, tostarp attiecībā uz ārpakalpojumu noteikumiem (kas reglamentē trešo personu, kas sniedz IKT pakalpojumus (*TPP*), uzraudzību); ļaut veikt kritiski svarīgu *TPP* IKT darbību pārraudzību; stimulēt apmaiņu ar draudu izlūkdatiem finanšu nozarē.

1.4.3. Paredzamie rezultāti un ietekme

Norādīt, kāda ir priekšlikuma/iniciatīvas iecerētā ietekme uz labuma guvējiem/mērķgrupām.

Digitālās darbības noturības akts finanšu nozarē nodrošinātu visaptverošu sistēmu, kas aptvertu visus digitālās darbības noturības aspektus un efektīvi uzlabotu finanšu nozares kopējo darbības noturību. Tas nodrošinātu vienotā noteikumu kopuma skaidrību un saskaņotību.

Tāpat tas padarītu skaidrāku un saskaņotāku mijiedarbību ar TID direktīvu, kā arī tās pārskatīšanu. Tas sniegtu finanšu vienībām skaidrību par dažādiem noteikumiem par digitālo darbības noturību, kas tām jāievēro, jo īpaši attiecībā uz tām finanšu vienībām, kurām ir vairākas atļaujas un kuras darbojas dažādos ES tirgos.

1.4.4. Snieguma rādītāji

Norādīt, pēc kādiem rādītājiem seko līdzi progresam un sasniegumiem.

Iespējamie rādītāji:

Ar IKT saistīto incidentu skaits ES finanšu nozarē un to ietekme

Būtisku ar IKT saistītu incidentu skaits, par kuriem ziņots prudenciālajiem uzraudzītājiem

Finanšu vienību skaits, kam būtu pienākums veikt draudu vadītus ielaušanās testus (DVIT).

Finanšu vienību skaits, kas izmanto līguma standartklauzulas, lai noslēgtu līgumiskas vienošanās ar IKT *TPP*

To kritiski svarīgo IKT *TPP* skaits, ko pārrauga EUI / prudenciālie uzraudzītāji

To finanšu vienību skaits, kas piedalās draudu izlūkdatu koplietošanas risinājumos

To iestāžu skaits, kam jāsaņem ziņojumi par vienu un to pašu ar IKT saistīto incidentu

Pārrobežu DVIT skaits

1.5. Priekšlikuma/iniciatīvas pamatojums

1.5.1. Īstermiņā vai ilgtermiņā izpildāmās vajadzības, tostarp sīki izstrādāts iniciatīvas izvēršanas grafiks

Finanšu nozarē tiek plaši izmantotas informācijas un komunikācijas tehnoloģijas (IKT). Neraugoties uz ievērojamo progresu, kas panākts, izmantojot mērķtiecīgu politiku un likumdošanas iniciatīvas valstu un Eiropas līmenī, IKT riski turpina sagādāt problēmas Savienības finanšu sistēmas noturībai, veiktspējai un stabilitātei. Pēc 2008. gada finanšu krīzes īstenotā reforma galvenokārt stiprināja ES finanšu nozares finansiālo noturību un tika veikta ar mērķi aizsargāt ES konkurētspēju un stabilitāti no ekonomiskā, prudenciālā un tirgus darbības viedokļa. IKT drošība un kopējā digitālās darbības noturība ir daļa no operacionālā riska, taču tām pēckrīzes regulatoru darba programmā ir veltīta mazāka uzmanība, un tās ir attīstītas tikai dažās Savienības finanšu tirgu politikas un regulējuma jomās vai tikai dažās dalībvalstīs. Tas rada šādas problēmas, kurus priekšlikumam vajadzētu risināt:

ES tiesiskais regulējums, kas attiecas uz visas finanšu nozares IKT risku un darbības noturību, ir sadrumstalots un nav pilnībā saskaņots.

Konsekventu prasību neesība ziņošanai par incidentiem, kas saistīti ar IKT, noved pie tā, ka uzraudzības iestādes nepilnīgi pārzina incidentu būtību, biežumu, nozīmīgumu un ietekmi.

Dažas finanšu vienības saskaras ar sarežģītām, atkārtotām un potenciāli nekonsekventām ziņošanas prasībām attiecībā uz vienu un to pašu ar IKT saistīto incidentu.

Nepietiekama informācijas apmaiņa un sadarbība kiberdraudu izlūkdatu jomā stratēģiskā, taktiskā un operatīvā līmenī liedz atsevišķām finanšu vienībām pienācīgi novērtēt un uzraudzīt kiberdraudus, kā arī aizstāvēties pret tiem un reaģēt uz tiem.

Dažās finanšu apakšnozarēs var pastāvēt vairāki nesaskaņoti ielaušanās un noturības testēšanas regulējumi, turklāt bez pārrobežu rezultātu atzīšanas, turpretī citās apakšnozarēs šāda testēšanas regulējuma nav.

Uzraudzības ieskatu trūkums attiecībā uz finanšu vienību darbībām, ko nodrošina IKT *TTP*, pakļauj operacionālajiem riskiem finanšu vienības atsevišķi un finanšu sistēmu kopumā.

Finanšu uzraudzības iestādes nav aprīkotas nedz ar pietiekamām pilnvarām, nedz rīkiem, kas ļautu uzraudzīt un pārvaldīt koncentrācijas un sistēmiskos riskus, ko rada finanšu vienību paļaušanās uz trešām personām IKT jomā.

1.5.2. Savienības iesaistīšanās pievienotā vērtība (tās pamatā var būt dažādi faktori, piemēram, koordinēšanas radītie ieguvumi, juridiskā noteiktība, lielāka rezultativitāte vai komplementaritāte). Šā punkta izpratnē "Savienības iesaistīšanās pievienotā vērtība" ir vērtība, kas veidojas Savienības iesaistīšanās rezultātā un kas papildina vērtību, kura veidotos, ja dalībvalstis rīkotos atsevišķi.

Eiropas līmeņa rīcības pamatojums (*ex ante*):

Digitālās darbības noturība ir ES finanšu tirgu kopīgo interešu jautājums. Rīcība ES līmenī sniegtu vairāk priekšrocību un lielāku pievienoto vērtību nekā atsevišķi valsts līmenī veikta rīcība. Nepievienojot IKT riska darbības noteikumus, vienotais noteikumu kopums gan nodrošinātu rīkus visu pārējo veidu risku novēršanai Eiropas līmenī, bet neiekļautu digitālās darbības noturības aspektus vai pakļautu tos sadrumstalotām un nekoordinētām valstu līmeņa iniciatīvām. Priekšlikums nodrošinātu juridisku skaidrību par to, vai un kā piemēro digitālās darbības noteikumus, jo īpaši attiecībā uz pārrobežu finanšu vienībām, un ar to tiktu novērsta nepieciešamība dalībvalstīm individuāli uzlabot noteikumus, standartus un gaidas attiecībā uz darbības noturību un kiberdrošību, reaģējot uz pašreizējo ierobežoto ES noteikumu tvērumu un TID direktīvas vispārējo būtību.

Gaidāmā Savienības pievienotā vērtība (*ex post*):

Savienības iejaukšanās būtiski palielinātu politikas efektivitāti, vienlaikus mazinot sarežģītību un atvieglojot finansiālo un administratīvo slogu visām finanšu vienībām. Ar to tiktu harmonizēta ekonomikas joma, kas ir dziļi savstarpēji savienota un integrēta un jau šobrīd izmanto vienotu noteikumu kopumu un uzraudzību. Ar IKT saistītu incidentu paziņošanas sakarā priekšlikums mazinātu ziņošanas slogu un aprēķinātās izmaksas, ko rada viena un tā paša ar IKT saistītā incidenta ziņošana dažādām ES un/vai valstu iestādēm. Tas arī sekmētu pāri robežām strādājošu iestāžu, kas dažādās dalībvalstīs ir pakļautas dažādam testēšanas regulējumam, testēšanas rezultātu savstarpēju atzīšanu un pieņemšanu.

1.5.3. Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas

Jauna iniciatīva

1.5.4. Saderība ar daudzgadu finanšu shēmu un iespējamā sinerģija ar citiem atbilstošiem instrumentiem

Šā priekšlikuma mērķis ir saskanīgs ar vairākiem citiem ES politikas pasākumiem un aktuālām iniciatīvām, jo īpaši Tīklu un informācijas drošības (TID) direktīvu un Eiropas kritiskās infrastruktūras (EKI) direktīvu. Ar priekšlikumu tiktu saglabāti ieguvumi, ko sniedz kiberdrošības horizontālais regulējums, saglabājot visas trīs finanšu apakšnozares TID direktīvas darbības jomā. Finanšu uzraudzības iestādes, saglabājot saistību ar TID ekosistēmu, spētu apmainīties ar attiecīgu informāciju ar TID iestādēm un piedalīties TID sadarbības grupā. Priekšlikums neietekmētu TID direktīvu, bet gan balstītos uz to un risinātu iespējamo pārklāšanos, izmantojot *lex specialis* atkāpi. Finanšu pakalpojumu direktīvas un TID direktīvas savstarpējai mijiedarbībai arī turpmāk piemērotu *lex specialis* klauzulu, tādējādi atbrīvojot finanšu vienības no TID direktīvas prasībām pēc būtības un izvairoties no abu tiesību aktu pārklāšanās. Turklāt priekšlikums ir saskanīgs ar Eiropas kritiskās infrastruktūras (EKI) direktīvu, kas patlaban tiek pārskatīta, lai uzlabotu kritiskās infrastruktūras aizsardzību un noturību pret draudiem, kas nav kiberdraudi.

Priekšlikums neietekmētu daudzgadu finanšu shēmu (DFS). Pirmkārt, kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, pārraudzības sistēma tiks pilnībā finansēta no maksām, ko iekasē no šiem pakalpojumu sniedzējiem; otrkārt, EUI uzticēto ar digitālās darbības noturību saistīto papildu regulatīvo uzdevumu izpildi nodrošinās esošā personāla iekšējā pārcelšana.

Tas izpaudīsies kā priekšlikums palielināt aģentūras pilnvaroto darbinieku skaitu nākamās ikgadējās budžeta procedūras laikā. Aģentūra turpinās strādāt, lai maksimāli palielinātu sinerģiju un efektivitātes pieaugumu (cita starpā izmantojot IT sistēmas), un cieši uzraudzīs ar šo priekšlikumu saistīto papildu darba slodzi, kas atspoguļosies aģentūras pieprasīto pilnvaroto darbinieku skaitā ikgadējā budžeta procedūrā.

1.5.5. Dažādo pieejamo finansēšanas iespēju, tostarp pārdales iespējas, novērtējums

Tika apsvērtas vairākas finansēšanas iespējas:

pirmkārt, papildu izmaksas varētu finansēt, izmantojot EUI parasto finansēšanas mehānismu. Tomēr tas prasību būtiski palielināt ES iemaksas EUI finanšu resursos.

Šī iespēja ir izvēlēta attiecībā uz izmaksām, kas saistītas ar šā priekšlikuma regulatīvo uzdevumu aspektiem. EUI tiks lūgtas pārcelt esošos darbiniekus, lai izstrādātu vairākus tehniskos standartus. Tomēr ar kritiski svarīgu TPP pārraudzību saistītās papildu izmaksas nevarētu segt, pārceļot EUI iekšējos resursus, kam bez šajā priekšlikumā un citos Savienības tiesību aktos paredzētajiem ir arī citi uzdevumi. Turklāt ar digitālās darbības noturību saistītie pārraudzības uzdevumi prasa īpašas tehniskās zināšanas un zinātību. Tā kā EUI šādu resursu pašreizējais apjoms ir nepietiekams, ir nepieciešami papildu resursi.

Visbeidzot, saskaņā ar priekšlikumu maksas tiks iekasētas no pārraudzībai pakļautajiem kritiski svarīgiem IKT *TPP*. Tās ir paredzētas, lai segtu visus papildu resursus, kas EUI ir nepieciešami jauno uzdevumu veikšanai un pilnvaru īstenošanai.

1.6. Priekšlikuma/iniciatīvas ilgums un finansiālā ietekme

☐ **ierobežots ilgums**

☐ Priekšlikuma/iniciatīvas darbības laiks: [DD.MM.]GGGG.–[DD.MM.]GGGG.

☐ Finansiālā ietekme: GGGG.– GGGG.

☑ **Beztermiņa**

Īstenošana ar uzsākšanas periodu no 2021. gada,

pēc kura turpinās normāla darbība.

1.7. Paredzētie pārvaldības veidi[51]

Tieša pārvaldība, īsteno Komisija ar

☐ izpildaģentūru starpniecību

☐ **Dalīta pārvaldība** kopā ar dalībvalstīm

☑ **Netieša pārvaldība**, kurā budžeta izpildes uzdevumi uzticēti:

☐ starptautiskām organizācijām un to aģentūrām (precizēt);

☐EIB un Eiropas Investīciju fondam;

☑ Finanšu regulas 70. un 71. pantā minētajām struktūrām;

☐ publisko tiesību subjektiem;

☐ privāttiesību subjektiem, kas veic valsts pārvaldes uzdevumus, ja tie sniedz pienācīgas finanšu garantijas;

☐ struktūrām, kuru darbību reglamentē dalībvalsts privāttiesības, kurām ir uzticēta publiskā un privātā sektora partnerības īstenošana un kuras sniedz pienācīgas finanšu garantijas;

☐ personām, kurām, ievērojot Līguma par Eiropas Savienību V sadaļu, uzticēts īstenot konkrētas KĀDP darbības un kuras ir noteiktas attiecīgajā pamataktā.

Piezīmes

NAV

[51] Sīkāku informāciju par pārvaldības veidiem un atsauces uz Finanšu regulu skatīt *BudgWeb* tīmekļa vietnē: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. PĀRVALDĪBAS PASĀKUMI

2.1. Pārraudzības un ziņošanas noteikumi

Norādīt biežumu un nosacījumus.

Saskaņā ar jau spēkā esošo kārtību EUI regulāri sagatavo ziņojumus par savu darbību (tostarp iekšējā ziņošana augstākajai vadībai, ziņošana valdēm un gada ziņojuma sagatavošana), un Revīzijas palāta un Komisijas Iekšējās revīzijas dienests veic revīzijas par tās resursu izmantošanu un darbības rezultātiem. Priekšlikumā iekļauto darbību uzraudzība un ziņošana atbildīs jau esošajām prasībām, kā arī visām jaunajām prasībām, kas izriet no šā priekšlikuma.

2.2. Pārvaldības un kontroles sistēma

2.2.1. Ierosināto pārvaldības veidu, finansējuma apgūšanas mehānismu, maksāšanas kārtības un kontroles stratēģijas pamatojums

Pārvaldība būs netieša, ar EUI starpniecību. Finansēšanas mehānismu īstenos, izmantojot maksas, ko iekasē no attiecīgajiem kritiski svarīgajiem IKT TPPS.

2.2.2. Informācija par apzinātajiem riskiem un risku mazināšanai izveidoto iekšējās kontroles sistēmu

Saistībā ar juridisku, ekonomisku, efektīvu un konstruktīvu apropriāciju izmantošanu, kas izriet no priekšlikuma, paredzams, ka priekšlikums neradīs jaunus būtiskus riskus, ko neaptver esošā iekšējās kontroles sistēma. Tomēr jauna problēma varētu būt saistīta ar maksas laicīgu iekasēšanu no attiecīgajiem IKT TPPS.

2.2.3. Kontroles izmaksefektivitātes (kontroles izmaksu attiecība pret attiecīgo pārvaldīto līdzekļu vērtību) aplēse un pamatojums un gaidāmā kļūdu riska līmeņa novērtējums (maksājumu izdarīšanas brīdī un slēgšanas brīdī)

Pārvaldības un kontroles sistēmas, kā noteikts EUI regulās, jau ir ieviestas. EUI cieši sadarbojas ar Komisijas Iekšējās revīzijas dienestu, lai nodrošinātu, ka attiecīgie standarti tiek ievēroti visās iekšējās kontroles sistēmas jomās. Saskaņā ar šo priekšlikumu šo kārtību piemēros arī attiecībā uz EUI lomu. Turklāt katru finanšu gadu Eiropas Parlaments pēc Padomes ieteikuma sniedz apstiprinājumu katrai EUI par budžeta izpildi.

2.3. Krāpšanas un pārkāpumu novēršanas pasākumi

Norādīt esošos vai plānotos novēršanas pasākumus un citus pretpasākumus, piemēram, krāpšanas apkarošanas stratēģijā iekļautos pasākumus.

Krāpšanas, korupcijas un citu nelikumīgu darbību apkarošanai EUI bez ierobežojumiem piemēro Eiropas Parlamenta un Padomes Regulu (ES, Euratom) Nr. 883/2013 (2013. gada 11. septembris) par izmeklēšanu, ko veic Eiropas Birojs krāpšanas apkarošanai (OLAF).

EUI ir īpaša krāpšanas apkarošanas stratēģija un no tās izrietošs rīcības plāns. EUI stiprinātas darbības krāpšanas apkarošanas jomā atbildīs noteikumiem un norādījumiem, kas sniegti Finanšu regulā (krāpšanas apkarošanas pasākumi kā daļa no pareizas finanšu pārvaldības), OLAF krāpšanas apkarošanas politikai, noteikumiem, kas paredzēti Komisijas krāpšanas apkarošanas stratēģijā (COM(2011) 376), kā arī izklāstīti kopējā pieejā par ES decentralizētajām aģentūrām (2012. gada jūlijs) un saistītajā ceļvedī.

Turklāt regulās, ar ko izveido EUI, kā arī EUI Finanšu regulās paredzēti noteikumi par EUI budžetu izpildi un kontroli un piemērojamie finanšu noteikumi, tostarp tie, kuru mērķis ir novērst krāpšanu un pārkāpumus.

3. PRIEKŠLIKUMA/INICIATĪVAS APLĒSTĀ FINANSIĀLĀ IETEKME

3.1. Attiecīgās daudzgadu finanšu shēmas izdevumu kategorijas un budžeta izdevumu pozīcijas

Esošās budžeta pozīcijas

Sarindotas pa daudzgadu finanšu shēmas izdevumu kategorijām un budžeta pozīcijām.

Daudzgadu finanšu shēmas izdevumu kategorija	Budžeta pozīcija	Izdevumu veids	Iemaksas			
	Skaits	Diff./Nedif f[52].	no EBTA valstīm[53]	no kandidātvalstīm[54]	no trešām valstīm	Finanšu regulas 21. panta 2. punkta b) apakšpunkta nozīmē

Jaunveidojamās budžeta pozīcijas

Sarindotas pa daudzgadu finanšu shēmas izdevumu kategorijām un budžeta pozīcijām.

Daudzgadu finanšu shēmas izdevumu kategorija	Budžeta pozīcija	Izdevumu veids	Iemaksas			
	Skaits	Dif./nedif.	no EBTA valstīm	no kandidātvalstīm	no trešām valstīm	Finanšu regulas 21. panta 2. punkta b) apakšpunkta nozīmē

[52] Dif. — diferencētās apropriācijas, nedif. — nediferencētās apropriācijas.

[53] EBTA: Eiropas Brīvās tirdzniecības asociācija.

[54] Kandidātvalstis un attiecīgā gadījumā potenciālās kandidātvalstis no Rietumbalkāniem.

3.2. Paredzamā ietekme uz izdevumiem

3.3. Kopsavilkums par paredzamo ietekmi uz izdevumiem

miljonos EUR (trīs zīmes aiz komata)

Daudzgadu finanšu shēmas izdevumu kategorija	Skaits	Pozīcija

ĢD : <..>			2020	2021	2022	2023	2024	2025	2026	2027	**KOPĀ**
	Saistības	(1)									
	Maksājumi	(2)									
KOPĀ ĢD <>	Saistības										
	Maksājumi										

Daudzgadu finanšu shēmas izdevumu kategorija		

miljonos EUR (trīs zīmes aiz komata)

		2022	2023	2024	2025	2026	2027	**KOPĀ**
ĢD:								
• Cilvēkresursi								
• Pārējie administratīvie izdevumi <>								
KOPĀ ĢD	Apropriācijas							

KOPĀ daudzgadu finanšu shēmas **IZDEVUMU KATEGORIJAS apropriācijas**	(Saistību summa = maksājumu summa)							

Miljonos EUR (līdz trim zīmēm aiz komata) salīdzināmās cenās

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**KOPĀ**
daudzgadu finanšu shēmas 1. IZDEVUMU KATEGORIJAS apropriācijas 1. IZDEVUMU KATEGORIJA	Saistības							
	Maksājumi							

3.3.1. Paredzamā ietekme uz apropriācijām

☑ Priekšlikumam/iniciatīvai nav vajadzīgas darbības apropriācijas

☐ Priekšlikums/iniciatīva paredz darbības apropriācijas izmantot šādā veidā:

Saistību apropriācijas miljonos EUR (3 zīmes aiz komata) salīdzināmās cenās

Norādīt mērķus un iznākumus ⇩			2022		2023		2024		2025		2026		2027		**KOPĀ**	
	Iznākumi															
	Veids[55]	Vidējās izmaksas	Nē	Izmaksas	Nē	Izmaksas	Nē	Izmaksas	Nē	Izmaksas	Nē	Izmaksas	Nē	Izmaksas	Kopējais daudzums	Kopējās izmaksas
KONKRĒTAIS MĒRĶIS Nr. 1[56] …																
– Rezultāts																
Starpsumma – konkrētais mērķis Nr. 1																
KONKRĒTAIS MĒRĶIS Nr. 2 ...																
– Rezultāts																
Starpsumma – konkrētais mērķis Nr. 2																
KOPĒJĀS IZMAKSAS																

55 Rezultāti ir piegādātie produkti vai pakalpojumi (piemēram, finansēto studentu apmaiņu skaits, uzbūvēto ceļu garums kilometros utt.).

56 Konkrētie mērķi, kas norādīti 1.4.2. punktā. "Konkrētie mērķi…".

3.3.2. Paredzamā ietekme uz cilvēkresursiem

3.3.2.1. Kopsavilkums

☐ Priekšlikums/iniciatīva neparedz izmantot administratīvās apropriācijas

☑ Priekšlikums/iniciatīva paredz izmantot administratīvās apropriācijas šādā veidā:

Miljonos EUR (līdz trim zīmēm aiz komata) salīdzināmās cenās

EBI, EAAPI, EVTI	2022	2023	2024	2025	2026	2027	**KOPĀ**
Pagaidu darbinieki (AD kategorijas)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Pagaidu darbinieki (AST kategorijas)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Līgumdarbinieki							
Pārceltie valsts eksperti							
KOPĀ	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Personāla vajadzības (PSE):

EBI, EAAPI, EVTI un EEZ	2022	2023	2024	2025	2026	2027	**KOPĀ**
Pagaidu darbinieki (AD kategorijas) EBI=5, EAAPI=5, EVTI=5	15	15	15	15	15	15	15
Pagaidu darbinieki (AST kategorijas) EBI=1, EAAPI=1, EEZ=1	3	3	3	3	3	3	3
Līgumdarbinieki							
Pārceltie valsts eksperti							

KOPĀ	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. Paredzamās cilvēkresursu vajadzības (atbildīgajam) ĢD

☑ Priekšlikumam/iniciatīvai nav vajadzīgi cilvēkresursi

☐ Priekšlikums/iniciatīva paredz cilvēkresursu izmantošanu šādā veidā:

Paredzamais apjoms izsakāms veselos skaitļos (vai maksimāli ar vienu zīmi aiz komata)

		2022	2023	2024	2025	2026	2027
• **Štatu sarakstā ietvertās amata vietas (ierēdņi un pagaidu darbinieki)**							
• **Ārštata darbinieki (izsakot ar pilnslodzes ekvivalentu – PSE)**[57]							
XX 01 02 01 (AC, END, INT, ko finansē no vispārīgajām apropriācijām)							
XX 01 02 02 (AC, AL, END, INT un JED delegācijās)							
XX 01 04 ***yy***[58]	— galvenajā mītnē[59]						
	— delegācijās						
XX 01 05 02 (*AC, END, INT* — netiešā pētniecība)							
10 01 05 02 (*AC, END, INT* — tiešā pētniecība)							
Citas budžeta pozīcijas (norādīt)							
KOPĀ							

XX ir attiecīgā politikas joma vai budžeta sadaļa.

Nepieciešamie cilvēkresursi tiks nodrošināti, izmantojot attiecīgā ĢD darbiniekus, kuri jau ir iesaistīti konkrētās darbības pārvaldībā un/vai ir pārgrupēti attiecīgajā ĢD, vajadzības gadījumā izmantojot arī vadošajam ĢD gada budžeta sadales procedūrā piešķirtos papildu resursus un ņemot vērā budžeta ierobežojumus.

Veicamo uzdevumu apraksts:

Ierēdņi un pagaidu darbinieki	
Ārštata darbinieki	

PSE vienību izmaksu aprēķins jāiekļauj 3. iedaļas V pielikumā.

57 AC – līgumdarbinieki, AL – vietējie darbinieki, SNE – valstu norīkotie eksperti, INT – aģentūru darbinieki, JED – jaunākie eksperti delegācijās.

58 Ārštata darbiniekiem paredzēto maksimālo summu finansē no darbības apropriācijām (kādreizējām BA pozīcijām).

59 Galvenokārt struktūrfondiem, Eiropas Lauksaimniecības fondam lauku attīstībai (ELFLA) un Eiropas Zivsaimniecības fondam (EZF).

3.3.3. Saderība ar pašreizējo daudzgadu finanšu shēmu

☑ Priekšlikums/iniciatīva atbilst kārtējai daudzgadu finanšu shēmai.

☐ Pieņemot priekšlikumu/iniciatīvu, jāpārplāno attiecīgā izdevumu kategorija daudzgadu finanšu shēmā.

☐ Pieņemot priekšlikumu/iniciatīvu, jāpiemēro elastības instruments vai jāpārskata daudzgadu finanšu shēma[60].

Paskaidrojiet, kas jādara, norādot attiecīgās izdevumu kategorijas, budžeta pozīcijas un atbilstošās summas. (..)

3.3.4. Trešo personu iemaksas

☐ Priekšlikums/iniciatīva neparedz trešo personu līdzfinansējumu.

☑ Priekšlikums/iniciatīva paredz šādu līdzfinansējumu:

miljonos EUR (trīs zīmes aiz komata)

EBI

	2022	2023	2024	2025	2026	2027	Kopā
Izmaksas 100 % apmērā sedz no maksām, ko iekasē no uzraudzītajām vienībām[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
KOPĀ līdzfinansētās apropriācijas	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EAAPI

	2022	2023	2024	2025	2026	2027	Kopā
Izmaksas 100 % apmērā sedz no maksām, ko iekasē no uzraudzītajām vienībām[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
KOPĀ līdzfinansētās apropriācijas	1,305	1,811	1,611	1,611	1,611	1,611	9,560

EVTI

	2022	2023	2024	2025	2026	2027	Kopā

60 Skatīt 11. un 17. pantu Padomes Regulā (ES, Euratom) Nr. 1311/2013, ar ko nosaka daudzgadu finanšu shēmu 2014.–2020. gadam.

61 100 % no kopējām paredzamajām izmaksām un pilnas darba devēja pensiju iemaksas.

62 100 % no kopējām paredzamajām izmaksām un pilnas darba devēja pensiju iemaksas.

Izmaksas 100 % apmērā sedz no maksām, ko iekasē no uzraudzītajām vienībām[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
KOPĀ līdzfinansētās apropriācijas	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Aplēstā ietekme uz ieņēmumiem

☑ Priekšlikums/iniciatīva ieņēmumus finansiāli neietekmē.

☐ Priekšlikums/iniciatīva finansiāli ietekmē:

☐ pašu resursus

☐ citus ieņēmumus

☐ Atzīmējiet, ja ieņēmumi ir piešķirti izdevumu pozīcijām

miljonos EUR (trīs zīmes aiz komata)

Budžeta ieņēmumu pozīcija:	Kārtējā finanšu gadā pieejamās apropriācijas	Priekšlikuma/iniciatīvas ietekme[64]						
		gads **N**	gads **N+1**	gads **N+2**	gads **N+3**	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)		
Pants …….								

Attiecībā uz īpaši "novirzāmiem" dažādajiem ieņēmumiem norādīt attiecīgo(-ās) izdevumu pozīciju(-as).

(..)

Norādīt ietekmes uz ieņēmumiem aprēķināšanai izmantoto metodi.

(..)

63 100 % no kopējām paredzamajām izmaksām un pilnas darba devēja pensiju iemaksas.

64 Norādītajām tradicionālo pašu resursu (muitas nodokļi, cukura nodevas) summām jābūt neto summām, t. i., bruto summām, no kurām atskaitītas iekasēšanas izmaksas 20 % apmērā.

PIELIKUMS

Vispārējie pieņēmumi

I sadaļa. Personāla izdevumi

Aprēķinot personāla izdevumus, pamatojoties uz identificēto nepieciešamo darbinieku skaitu, ir izmantoti šādi specifiski pieņēmumi:

- 2022. gadā darbā pieņemto papildu darbinieku izmaksas ir aprēķinātas par 6 mēnešiem, ņemot vērā pieļauto laiku, kas vajadzīgs papildu personāla pieņemšanai darbā
- Pagaidu darbinieka vidējās gada izmaksas ir 150 000 EUR, kas ietver 25 000 EUR no ekspluatācijas ("*habillage*") izmaksām (ēkas, IT utt.).
- Korekcijas koeficienti, kas piemērojami personāla algām Parīzē (EBI un EVTI) un Frankfurtē (EAAPI), ir attiecīgi 117,7 un 99,4
- Pagaidu darbinieku darba devēja pensiju iemaksas ir balstītas uz standarta pamatalgām, kas iekļautas standarta vidējās gada izmaksās, t. i., 95 660 EUR
- Papildu pagaidu darbinieki ir AD5 un AST.

II sadaļa. Infrastruktūras un darbības izdevumi

Izmaksas ir balstītas uz darbinieku skaita reizināšanu ar daļu no gada, kurā tie tikuši nodarbināti, un ar standarta izmaksām par ekspluatāciju ("*habillage*"), t. i., 25 000 EUR.

III sadaļa. Pamatdarbības izdevumi

Izmaksas tiek aprēķinātas, ievērojot šādus pieņēmumus:

- Tulkošanas izmaksas katrai EUI ir 350 000 EUR gadā
- Tiek pieņemts, ka katras EUI vienreizējās izmaksas 500 000 EUR apmērā tiks īstenotas no 2022. gada līdz 2023. gadam, sadalot tās 50 %–50 %. Ikgadējās uzturēšanas izmaksas no 2024. gada tiek lēstas 50 000 EUR apmērā uz EUI.
- Ikgadējās klātienes uzraudzības izmaksas tiek lēstas EUR 200 000 EUR apmērā uz EUI.

Iepriekš izklāstītās aplēses ļauj iegūt šādas izmaksas gadā:

Daudzgadu finanšu shēmas izdevumu kategorija	Skaits	

Pastāvīgās cenas

EBI:			2022	2023	2024	2025	2026	2027	**KOPĀ**
1. sadaļa:	Saistības	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Maksājumi	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
2. sadaļa:	Saistības	(1.a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Maksājumi	(2.a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
3. sadaļa:	Saistības	(3.a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Maksājumi	(3.b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
KOPĀ EBI	Saistības	=1+1.a +3.a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Maksājumi	=2+2.a +3.b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EAAPI:			2022	2023	2024	2025	2026	2027	**KOPĀ**
1. sadaļa:	Saistības	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Maksājumi	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
2. sadaļa:	Saistības	(1.a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Maksājumi	(2.a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
3. sadaļa:	Saistības	(3.a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Maksājumi	(3.b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
KOPĀ	Saistības	=1+1.a +3.a	1,305	1,811	1,611	1,611	1,611	1,611	9,560

EAAPI	Maksājumi	=2+2.a +3.b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

EVTI:			2022	2023	2024	2025	2026	2027	**KOPĀ**
1. sadaļa:	Saistības	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Maksājumi	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
2. sadaļa:	Saistības	(1.a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Maksājumi	(2.a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
3. sadaļa:	Saistības	(3.a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Maksājumi	(3.b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
KOPĀ EVTI	Saistības	=1+1.a +3.a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Maksājumi	=2+2.a +3.b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Priekšlikumam ir vajadzīgas šādas darbības apropriācijas:

Saistību apropriācijas miljonos EUR (3 zīmes aiz komata) salīdzināmās cenās

EBI

Norādīt mērķus un iznākumus ⇩			2022		2023		2024		2025		2026		2027			
	Iznākumi															
	Veids[65]	Vidējās izmaksas	Nē	Izmaksas	Nē	Izmaksas	Nē	Izmaksas	Nē	Izmaksas	Nē	Izmaksas	Nē	Izmaksas	Kopējais daudzums	Kopējās izmaksas
KONKRĒTAIS MĒRĶIS NR. 1 [66] Kritiski svarīgu IKT TPPS tiešā pārraudzība																
– Rezultāts				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Starpsumma – konkrētais mērķis Nr. 1																
KONKRĒTAIS MĒRĶIS Nr. 2 ...																
– Rezultāts																
Starpsumma – konkrētais mērķis Nr. 2																
KOPĒJĀS IZMAKSAS				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

EAAPI

Norādīt mērķus un iznākumus ⇩			2022		2023		2024		2025		2026		2027			
	Iznākumi															
	Veids[67]	Vidējās izmaksas	Nē	Izmaksas	Nē	Izmaksas	Nē	Izmaksas	Nē	Izmaksas	Nē	Izmaksas	Nē	Izmaksas	Kopējais daudzums	Kopējās izmaksas
KONKRĒTAIS MĒRĶIS NR. 1 [68] Kritiski svarīgu IKT TPPS tiešā pārraudzība																
– Rezultāts				0,800		0,800		0,600		0,600		0,600		0,600		4,000

[65] Rezultāti ir piegādātie produkti vai pakalpojumi (piemēram, finansēto studentu apmaiņu skaits, uzbūvēto ceļu garums kilometros utt.).

[66] Konkrētie mērķi, kas norādīti 1.4.2. punktā. "Konkrētie mērķi…".

[67] Rezultāti ir piegādātie produkti vai pakalpojumi (piemēram, finansēto studentu apmaiņu skaits, uzbūvēto ceļu garums kilometros utt.).

[68] Konkrētie mērķi, kas norādīti 1.4.2. punktā. "Konkrētie mērķi…".

Starpsumma – konkrētais mērķis Nr. 1															
KONKRĒTAIS MĒRĶIS Nr. 2 ...															
– Rezultāts															
Starpsumma – konkrētais mērķis Nr. 2															
KOPĒJĀS IZMAKSAS			**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

EVTI

Norādīt mērķus un iznākumus			2022		2023		2024		2025		2026		2027			
	Iznākumi															
⇩	Veids[69]	Vidējās izmaksas	Nē	Izmaksas	Nē	Izmaksas	Nē	Izmaksas	Nē	Izmaksas	Nē	Izmaksas	Nē	Izmaksas	Kopējais daudzums	Kopējās izmaksas
KONKRĒTAIS MĒRĶIS NR. 1 [70] Kritiski svarīgu IKT TPPS tiešā pārraudzība																
– Rezultāts				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Starpsumma – konkrētais mērķis Nr. 1																
KONKRĒTAIS MĒRĶIS Nr. 2 ...																
– Rezultāts																
Starpsumma – konkrētais mērķis Nr. 2																
KOPĒJĀS IZMAKSAS				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

[69] Rezultāti ir piegādātie produkti vai pakalpojumi (piemēram, finansēto studentu apmaiņu skaits, uzbūvēto ceļu garums kilometros utt.).

[70] Konkrētie mērķi, kas norādīti 1.4.2. punktā. "Konkrētie mērķi…".

Pārraudzības darbības pilnībā finansē no maksām, ko iekasē no uzraudzītajām vienībām šādi:

EBI

	2022	2023	2024	2025	2026	2027	Kopā
Izmaksas 100 % apmērā sedz no maksām, ko iekasē no uzraudzītajām vienībām[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
KOPĀ līdzfinansētās apropriācijas	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EAAPI

	2022	2023	2024	2025	2026	2027	Kopā
Izmaksas 100 % apmērā sedz no maksām, ko iekasē no uzraudzītajām vienībām[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
KOPĀ līdzfinansētās apropriācijas	1,305	1,811	1,611	1,611	1,611	1,611	9,560

EVTI

	2022	2023	2024	2025	2026	2027	Kopā
Izmaksas 100 % apmērā sedz no maksām, ko iekasē no uzraudzītajām vienībām[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
KOPĀ līdzfinansētās apropriācijas	1,373	1,948	1,748	1,748	1,748	1,748	10,313

ĪPAŠA INFORMĀCIJA

Tiešās pārraudzības pilnvaras

Vispirms jāatgādina, ka vienībām, ko tieši uzrauga EVTI, būtu jāveic maksas EVTI (vienreizējas izmaksas par reģistrāciju un regulāras izmaksas par pastāvīgu uzraudzību). Tas tā ir attiecībā uz

[71] 100 % no kopējām paredzamajām izmaksām un pilnas darba devēja pensiju iemaksas.
[72] 100 % no kopējām paredzamajām izmaksām un pilnas darba devēja pensiju iemaksas.
[73] 100 % no kopējām paredzamajām izmaksām un pilnas darba devēja pensiju iemaksas.

kredītreitingu aģentūrām (sk. Komisijas Deleģēto regulu (ES) Nr. 272/2012) un darījumu reģistriem (Komisijas Deleģētā regula (ES) Nr. 1003/2013).

Saskaņā ar šo tiesību akta priekšlikumu EUI tiks uzticēti jauni pienākumi, kuru mērķis ir sekmēt konverģenci attiecībā uz trešās personas, kas sniedz IKT pakalpojumus, riska finanšu nozarē uzraudzības pieeju, pakļaujot kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, Savienības pārraudzības sistēmai.

Ar šo regulu paredzētā pārraudzības sistēma ir balstīta uz esošo finanšu pakalpojumu nozares institucionālo sistēmu, kurā EUI Apvienotā komiteja nodrošina starpnozaru koordināciju visos ar IKT risku saistītajos jautājumos saskaņā ar uzdevumiem, kas tai uzticēti attiecībā uz kiberdrošību, bet tai atbalstu sniedz attiecīgā apakškomiteja (Pārraudzības forums), kas veic sagatavošanās darbu individuālu lēmumu un kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, adresēto kolektīvo ieteikumu pieņemšanai.

EUI, kas ir noteikta par katras šādas kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, galveno pārraugu, ar šo regulējumu iegūst pilnvaras nodrošināt, ka tehnoloģiju pakalpojumu sniedzēji, kam ir kritiski svarīga loma finanšu nozares darbībā, tiek pienācīgi uzraudzīti visas Eiropas mērogā. Pārraudzības pienākumi ir izklāstīti priekšlikumā un sīkāk precizēti paskaidrojuma rakstā. Tie ietver tiesībaspieprasīt visu attiecīgo informāciju un dokumentus, lai veiktu vispārīgas izmeklēšanas un pārbaudes, sniegt ieteikumus un pēc tam iesniegt ziņojumus par šo ieteikumu īstenošanai veiktajām darbībām vai īstenotajiem korektīvajiem pasākumiem.

Lai izpildītu šajā priekšlikumā paredzētos jaunos uzdevumus, EUI būtu jāpieņem darbā papildu darbinieki, kas specializējas IKT riska novērtēšanā un koncentrējas uz to, lai novērtētu atkarību no trešās personas.

Cilvēkresursu vajadzības ir aplēstas 6 pilnslodzes ekvivalentu apmērā katrai iestādei (5 AD un 1 AST, lai atbalstītu AD). EUI radīsies arī papildu IT izmaksas, kas aplēstas 500 000 EUR apmērā (vienreizējās izmaksas), kā arī 50 000 EUR gadā katrai no trim EUI par uzturēšanas izmaksām. Būtisks elements jauno uzdevumu izpildē ir apmeklējumi, lai veiktu pārbaudes uz vietas un revīzijas, ko katrai EUI var aplēst 200 000 EUR apmērā gadā. Tulkošanas izmaksas dažādiem dokumentiem, ko EUI saņemtu no kritiski svarīgajām trešām personām, kas sniedz IKT pakalpojumus, ir iekļautas arī darbības izmaksu ailē un ir 350 000 EUR gadā.

Visas minētās administratīvās izmaksas tiks pilnībā segtas no gada maksām, ko EUI iekasēs no uzraudzītajām trešām personām, kas sniedz IKT pakalpojumus (nav ietekmes uz ES budžetu).