I

(Leģislatīvi akti)

REGULAS

EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2022/2554

(2022. gada 14. decembris)

par finanšu nozares digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011

(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 valstu parlamentiem,

ņemot vērā Eiropas Centrālās bankas atzinumu ([1]),

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu ([2]),

saskaņā ar parasto likumdošanas procedūru ([3]),

tā kā:

(1) Informācijas un komunikācijas tehnoloģijas (IKT) digitālajā laikmetā atbalsta sarežģītas sistēmas, kas tiek lietotas ikdienas darbībām. Tās nodrošina mūsu ekonomikas darbību svarīgās nozarēs, tostarp finanšu nozarē, un uzlabo iekšējā tirgus darbību. Lielāka digitalizācija un savstarpēja savienojamība pastiprina arī IKT risku, padarot sabiedrību kopumā un jo īpaši finanšu sistēmu neaizsargātāku pret kiberdraudiem vai IKT traucējumiem. Lai gan plašais IKT sistēmu lietojums, augstā digitalizācija un savienojamība mūsdienās ir Savienības finanšu vienību veikto darbību pamatiezīmes, to digitālā noturība vēl ir pamatīgāk jāizskata un jāintegrē plašākos to darbības pamatprincipos.

(2) IKT izmantošana pēdējās desmitgadēs ir ieguvusi būtisku nozīmi finanšu pakalpojumu sniegšanā tādā mērā, ka tagad tā ir kļuvusi kritiski svarīga, lai veiktu parastas ikdienas darbības visās finanšu vienībās. Digitalizācija tagad 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, pretenziju apstrādi un biroja administratīvo darbu. Līdz ar IKT izmantošanu pārveidota ir arī apdrošināšanas nozare: sākot ar tādu apdrošināšanas starpnieku parādīšanos, kuri, darbojoties ar *InsurTech*, savus pakalpojumus piedāvā tiešsaistē, līdz

([1]) OV C 343, 26.8.2021., 1. lpp.
([2]) OV C 155, 30.4.2021., 38. lpp.
([3]) Eiropas Parlamenta 2022. gada 10. novembra nostāja (*Oficiālajā Vēstnesī* vēl nav publicēta) un Padomes 2022. gada 28. novembra lēmums.

tam, ka notiek digitāla apdrošināšanas saistību uzņemšanās. Ne tikai finanses visā nozarē ir kļuvušas digitālas, bet digitalizācija ir arī padarījusi intensīvākus 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 atkārtoti uzsvēra, kā sistēmisku ievainojamību varētu radīt tas, ka pastāv augsta līmeņa savstarpējā savienojamība starp finanšu vienībām, finanšu tirgiem un finanšu tirgus infrastruktūrām, jo īpaši savstarpēja to IKT sistēmu atkarība, jo vietēja mēroga kiberincidenti kādā no aptuveni 22 000 Savienības finanšu vienību varētu ātri izplatīties visā finanšu sistēmā, valstu robežām tos neaizkavējot. Smagi IKT pārkāpumi finanšu nozarē ietekmē ne tikai finanšu vienības atsevišķi. Tie arī atvieglo vietēja mēroga ievainojamības izplatīšanos finanšu sakaru kanālos un, iespējams, var radīt nelabvēlīgas sekas Savienības finanšu sistēmas stabilitātei, piemēram, izraisīt likviditātes pazemināšanos un kopumā mazināt pārliecību un uzticēšanos finanšu tirgiem.

(4) IKT risks pēdējos gados ir piesaistījis starptautisko, Savienības un valstu politikas veidotāju, regulatoru un standartu noteikšanas struktūru uzmanību, liekot tiem mēģināt uzlabot digitālo noturību, noteikt standartus, kā arī koordinēt regulatīvo 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 mērķis ir sniegt dažādu jurisdikciju kompetentajām iestādēm un tirgus dalībniekiem instrumentus savu finanšu sistēmu noturības stiprināšanai. Šā darba dzinulis bija arī vajadzība pienācīgi ņemt vērā IKT risku savstarpēji cieši saistītas globālās finanšu sistēmas kontekstā un tiekties pēc lielākas saskaņotības attiecīgajā paraugpraksē.

(5) Neraugoties uz mērķtiecīgu politiku un likumdošanas iniciatīvām Savienības un valstu līmenī, IKT risks turpina sagādāt problēmas Savienības finanšu sistēmas darbības noturībai, veiktspējai un stabilitātei. Reformas, kas tika īstenotas pēc 2008. gada finanšu krīzes, galvenokārt stiprināja Savienības finanšu nozares finansiālo noturību, un to mērķis bija 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 pēc finanšu krīzes izstrādātajā regulatoru darba programmā ir veltīta mazāka uzmanība, un tās ir attīstījušās tikai dažās Savienības finanšu pakalpojumu politikas un regulējošās vides jomās vai tikai dažās dalībvalstīs.

(6) Komisija 2018. gada 8. marta paziņojumā "Finanšu tehnoloģijas rīcības plāns konkurētspējīgākam un inovatīvākam Eiropas finanšu sektoram" uzsvēra, cik svarīgi ir padarīt Savienības finanšu nozari elastīgāku, tostarp no darbības perspektīvas, lai nodrošinātu tās tehnoloģisko drošību un labu darbību, ātru IKT pārkāpumu un incidentu seku novēršanu, un tas galu galā ļaus efektīvi un netraucēti sniegt finanšu pakalpojumus visā Savienībā, tostarp stresa situācijās, vienlaikus saglabājot patērētāju un tirgus uzticēšanos un paļāvību.

(7) 2019. gada aprīlī Eiropas Uzraudzības iestāde (Eiropas Banku iestāde), (EBI), kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1093/2010 ([4]), Eiropas Uzraudzības iestāde (Eiropas Apdrošināšanas un aroda pensiju iestāde), (EAAPI), kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 1094/2010 ([5]) un Eiropas Uzraudzības iestāde (Eiropas Vērtspapīru un tirgu iestāde), (EVTI), kas izveidota ar Eiropas Parlamenta un Padomes

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

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

Regulu (ES) Nr. 1095/2010 ([6]) (kopā zināmas kā "Eiropas uzraudzības iestādes", vai "EUI") kopīgi publicēja tehnisko ieteikumu, aicinot īstenot vienveidīgu pieeju IKT riskam finanšu nozarē un iesakot proporcionāli stiprināt finanšu pakalpojumu nozares digitālās darbības noturību ar nozarei specifisku Savienības iniciatīvu.

(8) Savienības finanšu nozare tiek regulēta ar 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, un nav mazāk svarīga, piemēram, par vienotiem prudenciālajiem vai tirgus rīcības standartiem. Tādēļ vienotais noteikumu kopums un uzraudzības sistēma būtu jāattīsta, lai tie aptvertu arī digitālās darbības noturību, šim nolūkam pastiprinot finanšu uzraudzības iestāžu pilnvaras, lai tās varētu uzraudzīt pārvaldību IKT risku finanšu nozarē ar mērķi aizsargāt iekšējā tirgus integritāti un efektivitāti un varētu sekmēt pienācīgu tā darbību.

(9) Tiesību aktu nesakritības un nevienāda valstu regulatīvā vai uzraudzības pieeja attiecībā uz IKT risku rada šķēršļus finanšu pakalpojumu iekšējā tirgus darbībai, finanšu vienībām, kas darbojas pāri robežām, apgrūtinot iedibinājumbrīvību un brīvību sniegt pakalpojumus. Varētu tikt kropļota arī konkurence starp viena veida finanšu vienībām, kas darbojas dažādās dalībvalstīs. Tas jo īpaši attiecas uz jomām, kurās saskaņošana Savienības līmenī ir bijusi ļoti ierobežota, piemēram, digitālās darbības noturības testēšanā, vai kurās tās nav bijis, piemēram, trešās personas IKT riska uzraudzība. Atšķirības, kas izriet no paredzamajām norisēm valstu līmenī, varētu radīt papildu šķēršļus iekšējā tirgus darbībai, tādējādi kaitējot tirgus dalībniekiem un finanšu stabilitātei.

(10) Tagad, tā kā ar IKT risku saistītie noteikumi Savienības līmenī ir izskatīti tikai daļēji, pastāv nepilnības vai pārklāšanās svarīgās jomās, piemēram ar IKT saistītu incidentu paziņošanā un digitālās darbības noturības testēšanā, un pretrunas, ko rada atšķirīgu valsts noteikumu rašanās vai izmaksu ziņā neefektīva tādu noteikumu piemērošana, kuri pārklājas. Tas jo īpaši nelabvēlīgi ietekmē tādu augstas IKT intensitātes 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 atļauja, kuru attiecīgi ir izdevušas dažādas kompetentās iestādes vienā vai vairākās dalībvalstīs), ir grūti pašām saskanīgi un izmaksu ziņā efektīvi novērst IKT risku un mazināt IKT incidentu nelabvēlīgo ietekmi.

(11) Tā kā vienotajam noteikumu kopumam nav pievienota visaptveroša IKT vai operacionālā riska sistēma, ir vēl jāsaskaņo galvenās prasības visu finanšu vienību digitālajai darbības noturībai. Tas, ka finanšu vienības, pamatojoties uz minētajām galvenajām prasībām, attīstītu IKT spējas un kopējo noturību nolūkā izturēt darbības pārtraukšanu, palīdzētu saglabāt Savienības finanšu tirgu stabilitāti un integritāti un tādējādi palīdzētu nodrošināt augsta līmeņa aizsardzību Savienības ieguldītājiem un patērētājiem. Tā kā šīs regulas mērķis ir veicināt netraucētu iekšējā tirgus darbību, tās pamatā vajadzētu būt Līguma par Eiropas Savienības darbību (LESD) 114. pantam saskaņā ar tā interpretāciju Eiropas Savienības Tiesas (Tiesa) pastāvīgajā judikatūrā.

(12) Šīs regulas mērķis ir konsolidēt un atjaunināt IKT riska prasības kā daļu no operacionālā riska prasībām, kuras līdz šim dažādos Savienības tiesību aktos ir aplūkotas atsevišķi. Šajos aktos ir aptvertas galvenās finanšu riska kategorijas (piem., kredītrisks, tirgus risks, darījuma partnera kredītrisks un likviditātes risks, tirgus uzvedības risks), tomēr to pieņemšanas laikā nav visaptveroši aplūkoti visi darbības noturības komponenti. Operacionālā riska noteikumos, kad tie tika sīkāk izstrādāti minētajos Savienības tiesību aktos, priekšroka bieži vien tika dota tradicionālai kvantitatīvajai riska novēršanas pieejai (proti, noteikt kapitāla prasību IKT riska segšanai), nevis paredzēti mērķtiecīgi kvalitatīvie noteikumi, ar kuriem nosaka spējas aizsargāt pret incidentiem, kas saistīti ar IKT, tos atklāt,

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

ierobežot, novērst to sekas un izlabot tos, vai ar kuriem nosaka ziņošanas un digitālās testēšanas spējas. Minētie akti galvenokārt bija paredzēti, lai aptvertu un atjauninātu būtiskākos prudenciālās uzraudzības, tirgus integritātes vai uzvedības noteikumus. Konsolidējot un atjauninot dažādos noteikumus par IKT risku, visiem noteikumiem, kas attiecas uz digitālo risku finanšu nozarē, vajadzētu pirmoreiz būt konsekventi apvienotiem vienā tiesību aktā. Tāpēc šajā regulā tiek novērstas nepilnības vai pretrunas dažos iepriekšējos tiesību aktos, tostarp attiecībā uz tajos izmantoto terminoloģiju, un tajā ir dotas skaidras atsauces uz IKT risku, izmantojot mērķtiecīgus noteikumus par IKT riska pārvaldības spējām, incidentu paziņošanu, darbības noturības testēšanu, kā arī ar trešo personu saistītā IKT riska uzraudzību. Tādējādi ar šo regulu būtu arī jāveicina informētība par IKT risku, un tajā būtu jāatzīst, ka IKT incidenti un darbības noturības trūkums var apdraudēt finanšu vienību stabilitāti.

(13) Finanšu vienībām IKT riska novēršanā būtu jāievēro vienāda pieeja un vienādi uz principiem balstīti noteikumi, ņemot vērā savu lielumu un vispārējo riska profilu, kā arī savu pakalpojumu, darbību un operāciju veidu, apmēru un sarežģītību. Konsekvence veicina uzticēšanos finanšu sistēmai un tās stabilitātes saglabāšanu, īpaši laikā, kad ir ļoti liela paļaušanās uz IKT sistēmām, platformām un infrastruktūru, kas rada lielāku digitālo risku. Ievērojot kiberhigiēnas pamatus, būtu arī jāizvairās no augstu izmaksu rašanās tautsaimniecībai, pēc iespējas samazinot IKT traucējumu ietekmi un izmaksas.

(14) Regula palīdz samazināt regulējuma sarežģītību, sekmē uzraudzības konverģenci un palielina juridisko noteiktību, kā arī veicina atbilstības nodrošināšanas izmaksu ierobežošanu, 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, ir vispiemērotākais veids, kā nodrošināt viendabīgu un saskaņotu visu IKT riska pārvaldības komponentu piemērošanu Savienības finanšu nozarē.

(15) Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 ([7]) bija pirmais horizontālais kiberdrošības regulējums, kas ir ieviests Savienības līmenī un tiek piemērots arī trim finanšu vienību veidiem, proti, kredītiestādēm, tirdzniecības vietām un centrālajiem darījumu partneriem. Tomēr, tā kā Direktīvā (ES) 2016/1148 ir paredzēts mehānisms, kā valsts līmenī identificēt pamatpakalpojumu sniedzējus, tikai dažas kredītiestādes, tirdzniecības vietas un centrālie darījumu partneri, ko dalībvalstis ir identificējušas, praksē ir iekļautas direktīvas darbības jomā, un līdz ar to no tām tiek prasīts ievērot tajā noteiktās IKT drošības un incidentu paziņošanas prasības. Eiropas Parlamenta un Padomes Direktīvā (ES) 2022/2555 ([8]) ir paredzēts vienots kritērijs, lai noteiktu vienības, kas ietilpst tās piemērošanas jomā (lieluma ierobežošanas noteikums), vienlaikus arī tās darbības jomā saglabājot trīs finanšu vienību veidus.

(16) Tomēr, tā kā šī regula paaugstina dažādo digitālās noturības komponentu saskaņošanas līmeni, ieviešot prasības attiecībā uz IKT riska pārvaldību un ar IKT saistītu incidentu paziņošanu, kuras ir stingrākas salīdzinājumā ar spēkā esošajos Savienības finanšu pakalpojumu tiesību aktos noteiktajām prasībām, šis augstākais līmenis nozīmē arī lielāku saskaņošanu salīdzinājumā ar Direktīvā (ES) 2022/2555 prasībām. Tādēļ šī regula attiecībā pret Direktīvu (ES) 2022/2555 ir *lex specialis*. Vienlaikus ir svarīgi saglabāt stingru saikni starp finanšu nozari un Savienības horizontālo kiberdrošības regulējumu, kas tagad ir izklāstīts Direktīvā (ES) 2022/2555, lai nodrošinātu saskaņu ar dalībvalstu pieņemtajām kiberdrošības stratēģijām un lai ļautu finanšu uzraudzības iestādēm apzināties kiberincidentus, kas ietekmē citas nozares, uz kurām attiecas minētā direktīva.

([7]) 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.).

([8]) Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris) par pasākumiem nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva) (skatīt šā *Oficiālā Vēstneša* 80.. lpp.).

(17) Saskaņā ar 4. panta 2. punktu Līgumā par Eiropas Savienību un neskarot pārskatīšanu Tiesā, šai regulai nebūtu jāietekmē dalībvalstu atbildība par valsts pamatfunkciju īstenošanu sabiedriskās drošības, aizsardzības un valsts drošības aizsardzības jomā, piemēram, attiecībā uz tādas informācijas sniegšanu, kas būtu pretrunā valsts drošības aizsardzībai.

(18) Lai nodrošinātu starpnozaru mācīšanos un efektīvi izmantotu citu nozaru pieredzi kiberdraudu novēršanā, Direktīvā (ES) 2022/2555 minētajām finanšu vienībām arī turpmāk vajadzētu būt daļai no minētās direktīvas "ekosistēmas" (piemēram, Sadarbības grupai un datordrošības incidentu reaģēšanas vienībām (*CSIRT*)). EUI un valstu kompetentajām iestādēm būtu jāspēj piedalīties stratēģiskās politikas apspriedēs un sadarbības grupas tehniskajā darbā saskaņā ar minēto direktīvu un apmainīties ar informāciju un turpināt sadarboties ar vienotajiem kontaktpunktiem, kas izraudzīti vai izveidoti saskaņā ar minēto direktīvu. Kompetentajām iestādēm saskaņā ar šo regulu būtu arī jākonsultējas un jāsadarbojas ar *CSIRT*. Kompetentajām iestādēm būtu jāspēj arī lūgt tehniskus ieteikumus no kompetentajām iestādēm, kas izraudzītas vai izveidotas saskaņā ar Direktīvu (ES) 2022/2555, un slēgt sadarbības vienošanās, kuru mērķis ir nodrošināt efektīvus un ātras reakcijas koordinācijas mehānismus.

(19) Tā kā finanšu vienību digitālā un fiziskā noturība ir cieši saistītas, šajā regulā un Eiropas Parlamenta un Padomes Direktīvā (ES) 2022/2557 ([9]) ir vajadzīga saskaņota pieeja attiecībā uz kritisko vienību noturību. Tā kā finanšu vienību fiziskā noturība ir visaptveroši izskatīta šīs regulas darbības jomā esošajos IKT riska pārvaldības un ziņošanas pienākumos, Direktīvas (ES) 2022/2557 III un IV nodaļā noteiktie pienākumi nebūtu jāpiemēro finanšu vienībām, uz kurām attiecas minētās direktīvas darbības joma.

(20) Mākoņdatošanas pakalpojumu sniedzēji ir viena no tām digitālo infrastruktūru kategorijām, uz kurām attiecas Direktīva (ES) 2022/2555. Ar šo regulu izveidotā Savienības pārraudzības sistēma (pārraudzības sistēma) attiecas uz visām kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, tostarp mākoņdatošanas pakalpojumu sniedzējiem, kas sniedz IKT pakalpojumus finanšu vienībām, un būtu jāuzskata, ka tā papildina uzraudzību, ko veic, ievērojot Direktīvu (ES) 2022/2555. Turklāt ar šo regulu izveidotajai pārraudzības sistēmai būtu jāattiecas uz mākoņdatošanas pakalpojumu sniedzējiem gadījumā, ja nav Savienības horizontālās sistēmas, ar ko izveido digitālo pārraudzības iestādi.

(21) Lai turpinātu pilnībā kontrolēt IKT risku, finanšu vienībām ir jābūt visaptverošām spējām, kas nodrošina spēcīgu un efektīvu IKT riska pārvaldību, kā arī īpašiem visu ar IKT saistītu incidentu novēršanas un nozīmīgāko ar IKT saistītu incidentu paziņošanas mehānismiem un politikai. Tāpat finanšu vienībām būtu jāievieš politika IKT sistēmu, kontroles un procesu testēšanai, kā arī trešo personu IKT riska pārvaldībai. Būtu jāpaaugstina finanšu vienību digitālās darbības noturības pamatlīmenis, vienlaikus ļaujot arī samērīgi piemērot prasības dažām finanšu vienībām, jo īpaši mikrouzņēmumiem, kā arī tām finanšu vienībām, uz kurām attiecas vienkāršota IKT riska pārvaldības sistēma. Lai veicinātu efektīvu arodpensijas kapitāla uzkrāšanas institūciju uzraudzību, kas ir samērīga un pievēršas nepieciešamībai samazināt administratīvo slogu kompetentajām iestādēm, attiecīgajos valsts uzraudzības pasākumos attiecībā uz šādām finanšu vienībām būtu jāņem vērā to lielums un vispārējais riska profils, kā arī to pakalpojumu, darbību un operāciju veids, apmērs un sarežģītība pat tad, ja ir pārsniegtas attiecīgās robežvērtības, kas noteiktas Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/2341 ([10]) 5. pantā. Jo īpaši uzraudzības darbībās galvenā uzmanība būtu jāpievērš vajadzībai novērst nopietnus riskus, kas saistīti ar konkrētas vienības IKT riska pārvaldību.

([9]) Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2557 (2022. gada 14. decembris) par kritisko vienību noturību un ar ko atceļ Padomes Direktīvu 2008/114/EK (skatīt šā *Oficiālā Vēstneša* 164. lpp.).

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

Kompetentajām iestādēm būtu arī jāsaglabā modra, bet samērīga pieeja attiecībā uz arodpensijas kapitāla uzkrāšanas institūciju uzraudzību, kuras saskaņā ar Direktīvas (ES) 2016/2341 31. pantu būtisku savas pamatdarbības daļu, piemēram, aktīvu pārvaldību, aktuāraprēķinus, grāmatvedību un datu pārvaldību, nodod ārpakalpojumu sniedzējiem.

(22) Ar IKT saistīto incidentu paziņošanas robežvērtības un taksonomija valstu līmenī ievērojami atšķiras. Lai gan pie kopsaucēja var nonākt ar attiecīgo darbu, ko saskaņā ar Direktīvu (ES) 2022/2555 veic Eiropas Savienības Kiberdrošības aģentūra (*ENISA*), kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) 2019/881 ([11]), un sadarbības grupa, pārējām finanšu vienībām joprojām pastāv vai var rasties atšķirīgas pieejas attiecībā uz robežvērtību noteikšanu un taksonomijas izmantošanu. Minēto atšķirību dēļ pastāv vairākas prasības, kas finanšu vienībām jāievēro, īpaši tad, kad tās darbojas vairākās dalībvalstīs un kad tās ir finanšu grupas daļa. Turklāt šādas atšķirības rada iespēju kavēt vēl vienotāku vai centralizētu Savienības mehānismu izveidi, kuri paātrina ziņošanas procesu un atbalsta ātru un vienmērīgu informācijas apmaiņu starp kompetentajām iestādēm, kas ir būtiski IKT riska novēršanai liela mēroga uzbrukumu gadījumā ar potenciāli sistēmiskām sekām.

(23) Lai samazinātu administratīvo slogu un iespējamu ziņošanas pienākumu dublēšanos dažām finanšu vienībām, incidentu paziņošanas prasība, ievērojot Eiropas Parlamenta un Padomes Direktīvu (ES) 2015/2366 ([12]), vairs nebūtu jāpiemēro maksājumu pakalpojumu sniedzējiem, uz kuriem attiecas šīs regulas darbības joma. Tādēļ kredītiestādēm, elektroniskās naudas iestādēm, maksājumu iestādēm un konta informācijas pakalpojumu sniedzējiem, kā norādīts minētās direktīvas 33. panta 1. punktā, ievērojot šo regulu, būtu no šīs regulas piemērošanas dienas jāziņo par visiem ar maksājumiem saistītiem darbības vai drošības incidentiem, par kuriem iepriekš tika ziņots, ievērojot minēto direktīvu, neatkarīgi no tā, vai šādi incidenti ir saistīti ar IKT.

(24) Lai kompetentās iestādes varētu pildīt uzraudzības uzdevumus, gūstot 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, šajā regulā būtu jāparedz stabila ar IKT saistītu incidentu paziņošanas kārtība, kurā ar attiecīgām prasībām novērš pašreizējās nepilnības finanšu pakalpojumu tiesību aktos un novērstu pašreizējos pārklāšanās un dublēšanās gadījumus, lai mazinātu izmaksas. Ir svarīgi saskaņot ar IKT saistītu incidentu paziņošanas kārtību, visām finanšu vienībām prasot iesniegt ziņojumus savām kompetentajām iestādēm vienotā, racionalizētā sistēmā, kā izklāstīts šajā regulā. Turklāt EUI būtu jāpilnvaro sīkāk noteikt būtiskus ar IKT saistīto incidentu paziņošanas sistēmas elementus, piemēram, taksonomiju, termiņus, datu kopas, veidnes un piemērojamās robežvērtības. Lai nodrošinātu pilnīgu saskaņotību ar Direktīvu (ES) 2022/2555, finanšu vienībām būtu jāļauj brīvprātīgi paziņot attiecīgajai kompetentajai iestādei par būtiskiem kiberdraudiem, ja tās uzskata, ka kiberdraudi ir būtiski finanšu sistēmai, pakalpojumu lietotājiem vai klientiem.

(25) Dažās finanšu apakšnozarēs ir izstrādātas digitālās darbības noturības testēšanas prasības, nosakot sistēmas, kas ne vienmēr ir pilnībā saskaņotas. Tā rezultātā pārrobežu finanšu vienībām var rasties izmaksu dublēšanās un tiek sarežģīta savstarpēja digitālās darbības noturības testēšanas rezultātu atzīšana, un tas savukārt var sadrumstalot iekšējo tirgu.

([11]) 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.).

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

(26) Turklāt, ja IKT testēšana netiek prasīta, ievainojamība paliek neatklāta un tā rezultātā finanšu vienība tiek pakļauta IKT riskam, un galu galā rodas lielāks risks finanšu nozares stabilitātei un integritātei. Bez Savienības iejaukšanās digitālās darbības noturības testēšana arī turpmāk būtu nekonsekventa un trūktu sistēmas savstarpējai IKT testēšanas rezultātu atzīšanai dažādās jurisdikcijās. Turklāt, tā kā ir maz ticams, ka citas finanšu apakšnozares nozīmīgā apmērā pieņemtu testēšanas shēmas, tās zaudētu iespējamos ieguvumus no testēšanas sistēmas attiecībā uz IKT ievainojamību un risku atklāšanu, un aizsardzības spēju un darbības nepārtrauktības testēšanu, kas palīdz vairot klientu, piegādātāju un darījumu partneru uzticēšanos. Lai novērstu minēto pārklāšanos, atšķirības un nepilnības, ir jāparedz noteikumi koordinētai testēšanas kārtībai un tādējādi jāatvieglo savstarpēja pastiprinātas testēšanas atzīšana, kuru veic tām finanšu vienībām, kuras atbilst šajā regulā izklāstītiem kritērijiem.

(27) Finanšu vienību paļaušanos uz IKT pakalpojumu izmantošanu daļēji nosaka to nepieciešamība pielāgoties jaunai konkurencei digitālajā globālajā ekonomikā, celt uzņēmējdarbības efektivitāti un apmierināt klientu pieprasījumu. Šādas paļaušanās veids un apmērs pēdējo gadu laikā ir pastāvīgi mainījies, sekmējot finanšu starpniecības izmaksu samazināšanos, ļaujot uzņēmumiem paplašināties un mērogot finanšu darbību izvēršanu, vienlaikus piedāvājot plašu IKT rīku klāstu sarežģītu iekšējo procesu pārvaldībai.

(28) Plašo IKT pakalpojumu izmantošanu apliecina sarežģītas līgumiskas vienošanās, kuru kontekstā finanšu vienībām bieži rodas grūtības vienoties par līguma noteikumiem, kas būtu pielāgoti prudenciālajiem standartiem vai citām regulatīvām prasībām, kas tām jāievēro, vai citādi īstenot īpašas tiesības, piemēram, piekļuves tiesības vai revīzijas tiesības, pat ja to līgumiskās vienošanās tādas paredz. Turklāt daudzas minētās līgumiskās vienošanās neparedz pietiekamus aizsardzības pasākumus, kas ļautu pilnībā uzraudzīt apakšuzņēmuma līguma slēgšanas procesus, tādējādi liedzot finanšu vienībai spēju novērtēt ar to saistītos riskus. Turklāt, tā kā trešās personas, kas ir IKT pakalpojumu sniedzējas, bieži sniedz standartizētus pakalpojumus dažādu veidu klientiem, šādas līgumiskas vienošanās ne vienmēr pienācīgi atbilst individuālām vai īpašām finanšu nozares dalībnieku vajadzībām.

(29) Lai arī Savienības tiesību aktos par finanšu pakalpojumiem ir daži vispārīgi noteikumi par ārpakalpojumiem, 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 jānosaka daži pamatprincipi, pēc kuriem finanšu vienības vadītos attiecībā uz trešo personu IKT risku un kuri ir īpaši svarīgi, ja finanšu vienības izmanto trešās personas, kas sniedz IKT pakalpojumus, savu kritiski svarīgo vai svarīgo funkciju atbalstam. Minētie principi būtu jāpapildina ar līgumisko pamattiesību kopumu attiecībā uz vairākiem līgumisko vienošanos izpildes un izbeigšanas elementiem konkrētu minimālo aizsardzības pasākumu nodrošināšanai, lai stiprinātu finanšu vienības spēju efektīvi uzraudzīt visu IKT risku, kas rodas to trešo personu līmenī, kuras sniedz pakalpojumus. Minētie principi papildina nozaru tiesību aktus, ko piemēro ārpakalpojumiem.

(30) Pašlaik pastāv zināms viendabības un konverģences trūkums attiecībā uz to, kā tiek uzraudzīts ar trešo personu saistītais IKT risks un trešo personu atkarība no IKT. Neraugoties uz tādiem centieniem risināt ārpakalpojumu jautājumu kā EBI 2019. gada pamatnostādnes par ārpakalpojumu izmantošanu un EVTI 2021. gada pamatnostādnes par ārpakalpojumu nodošanu mākoņpakalpojumu sniedzējiem, plašākais jautājums par vēršanos pret sistēmisku risku, ko varētu izraisīt finanšu nozares pakļautība ierobežotam skaitam kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, Savienības tiesību aktos nav pietiekami aplūkots. Noteikumu trūkumu Savienības līmenī saasina tas, ka nav valstu noteikumu par pilnvarojumiem un rīkiem, kas ļautu finanšu uzraudzības iestādēm iegūt labu izpratni par atkarību no trešām personām, kas sniedz IKT pakalpojumus, un pienācīgi uzraudzīt riskus, ko rada koncentrēta atkarība no trešām personām, kas sniedz IKT pakalpojumus.

(31) Ņemot vērā iespējamo sistēmisko risku, ko rada ārpakalpojumu izmantošanas prakse un IKT trešo personu koncentrācija, un paturot prātā to, ka valstu mehānismi nav pietiekami, lai finanšu uzraudzības iestādēm nodrošinātu pienācīgus rīkus, ar ko kvantitatīvi noteikt, kvalificēt un novērst tāda IKT riska sekas, kas rodas kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, ir jāizveido pienācīga pārraudzības sistēma, kas ļautu pastāvīgi uzraudzīt to trešo personu darbības, kuras sniedz IKT pakalpojumus, kas ir kritiski svarīgi pakalpojumu sniedzēji finanšu vienībām, vienlaikus nodrošinot klientu un citu finanšu vienību konfidencialitātes un drošības saglabāšanu. Lai gan IKT pakalpojumu sniegšana grupas iekšienē rada īpašus riskus un ieguvumus, nevajadzētu automātiski uzskatīt, ka tā nav tik riskanta kā IKT pakalpojumu sniegšana, ko īsteno pakalpojumu sniedzēji ārpus finanšu grupas, un tāpēc uz to būtu jāattiecina tas pats tiesiskais regulējums. Tomēr, ja IKT pakalpojumi tiek sniegti vienā un tajā pašā finanšu grupā, finanšu vienības pakalpojumu sniedzējus grupas iekšienē varētu kontrolēt augstākā līmenī, un tas būtu jāņem vērā vispārējā riska novērtējumā.

(32) Tā kā IKT risks kļūst arvien sarežģītāks un attīstītāks, labi pasākumi IKT riska atklāšanai un profilaksei lielākoties ir atkarīgi no regulāras apdraudējumu un ievainojamības izlūkdatu apmaiņas starp finanšu vienībām. Informācijas apmaiņa veicina lielākas izpratnes veidošanu par kiberdraudiem. Tas savukārt uzlabo finanšu vienību spēju novērst kiberdraudu pārtapšanu reālos ar IKT saistītos incidentos un ļauj finanšu vienībām efektīvāk ierobežot ar IKT saistīto incidentu ietekmi un ātrāk novērst to sekas. Tā kā nepastāv Savienības līmeņa norādījumi, šādu izlūkdatu apmaiņu, šķiet, ir kavējuši vairāki faktori, jo īpaši nenoteiktība attiecībā uz tās saderību ar datu aizsardzības, pretmonopola un atbildības noteikumiem.

(33) 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 Eiropolu – tiesībaizsardzības mērķiem). Tādēļ patlaban informācijas apmaiņas apjoms un kvalitāte joprojām ir ierobežoti un sadrumstaloti, attiecīgā apmaiņa pārsvarā tiek veikta vietējā līmenī (izmantojot valstu iniciatīvas), un nepastāv konsekventa Savienības mēroga informācijas apmaiņas kārtība, kas būtu pielāgota integrētas finanšu sistēmas vajadzībām. Šajā sakarā ir svarīgi stiprināt minētos saziņas kanālus.

(34) Finanšu vienības būtu jāmudina savstarpēji apmainīties ar informāciju par kiberdraudiem un ar izlūkdatiem un 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, piedaloties informācijas apmaiņas pasākumos. Tādēļ ir nepieciešams ļaut Savienības līmenī rasties mehānismiem, kuri paredz brīvprātīgu informācijas apmaiņas kārtību un kuri, veikti uzticamā vidē, palīdzēs finanšu nozares kopienai novērst kiberdraudus un kolektīvi reaģēt uz tiem, ātri ierobežojot IKT riska izplatīšanos un kavējot iespējamu kaitīgas ietekmes izplatīšanos pa finanšu kanāliem. Minētajiem mehānismiem būtu jāatbilst piemērojamajiem Savienības konkurences tiesību noteikumiem, kas izklāstīti Komisijas 2011. gada 14. janvāra paziņojumā "Pamatnostādnes par Līguma par Eiropas Savienības darbību 101. panta piemērojamību horizontālās sadarbības nolīgumiem", kā arī Savienības datu aizsardzības noteikumiem, jo īpaši Eiropas Parlamenta un Padomes Regulai (ES) 2016/679 ([13]). Minētajiem mehānismiem būtu jādarbojas, pamatojoties uz viena vai vairāku minētās regulas 6. pantā noteikto juridisko pamatu izmantošanu, piemēram, saistībā ar minētās regulas 6. panta 1. punkta f) apakšpunktā minēto personas datu apstrādi, kas ir nepieciešama pārziņa vai trešās personas leģitīmo interešu ievērošanai, kā arī saistībā ar personas datu apstrādi, kas ir nepieciešama, lai izpildītu uz pārzini attiecināmas juridiskas saistības, un kas ir vajadzīga, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim likumīgi piešķirtās oficiālās pilnvaras, kā attiecīgi norādīts minētās regulas 6. panta 1. punkta c) un e) apakšpunktā.

([13]) 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.).

(35) Lai saglabātu augstu digitālās darbības noturības līmeni visā finanšu nozarē un vienlaikus ietu kopsolī ar tehnoloģiju attīstību, ar šo regulu būtu jānovērš risks, kas izriet no visu veidu IKT pakalpojumiem. Šajā nolūkā IKT pakalpojumu definīcija šīs regulas kontekstā būtu jāsaprot plaši, ietverot digitālos un datu pakalpojumus, ko ar IKT sistēmu starpniecību pastāvīgi sniedz vienam vai vairākiem iekšējiem vai ārējiem lietotājiem. Minētajai definīcijai, piemēram, būtu jāietver tā sauktie *OTT* (*over the top*) pakalpojumi, kas ietilpst elektronisko komunikāciju pakalpojumu kategorijā. Tajā nebūtu jāietver tikai ierobežota tādu tradicionālo analogās telefonijas pakalpojumu kategorija, kuri kvalificējami kā publiskā komutējamā telefonu tīkla (*PSTN*) pakalpojumi, fiksētā tīkla pakalpojumi, analogā balss telefonijas pieslēguma pakalpojumi (*POTS*) vai fiksētās telefonijas pakalpojumi.

(36) Neraugoties uz šajā regulā paredzēto plašo darbības jomu, piemērojot digitālās darbības noturības noteikumus, būtu jāņem vērā nozīmīgas atšķirības attiecībā uz finanšu vienību lielumu un vispārējo riska profilu. Vispārīgs princips paredz, ka finanšu vienībām, sadalot resursus un spējas IKT riska pārvaldības sistēmas īstenošanai, ar IKT saistītās vajadzības būtu pienācīgi jālīdzsvaro ar to lielumu un vispārējo riska profilu un to pakalpojumu, darbību un operāciju veidu, apmēru un sarežģītību, savukārt kompetentajām iestādēm būtu jāturpina vērtēt un pārskatīt šādas sadales pieeju.

(37) Konta informācijas pakalpojumu sniedzēji, kas minēti Direktīvas (ES) 2015/2366 33. panta 1. punktā, ir nepārprotami iekļauti šīs regulas darbības jomā, ņemot vērā to darbības veidu un ar to saistītos riskus. Turklāt elektroniskās naudas iestādes un maksājumu iestādes, kurām piemēro izņēmumu, ievērojot Eiropas Parlamenta un Padomes Direktīvas 2009/110/EK ([14]) 9. panta 1. punktu un Direktīvas (ES) 2015/2366 32. panta 1. punktu, ir iekļautas šīs regulas darbības jomā, pat ja tām saskaņā ar Direktīvu 2009/110/EK nav piešķirta atļauja emitēt elektronisko naudu vai ja tām saskaņā ar Direktīvu (ES) 2015/2366 nav piešķirta atļauja sniegt un izpildīt maksājumu pakalpojumus. Tomēr šīs regulas darbības jomā nav iekļautas pasta žiro norēķinu iestādes, kas minētas Eiropas Parlamenta un Padomes Direktīvas 2013/36/ES ([15]) 2. panta 5. punkta 3. apakšpunktā. Kompetentajai iestādei, ko izraugās maksājumu iestādēm, kam piemēro izņēmumu, ievērojot Direktīvu (ES) 2015/2366, elektroniskās naudas iestādēm, kam piemēro izņēmumu, ievērojot Direktīvu 2009/110/EK, un konta informācijas pakalpojumu sniedzējiem, kas minēti Direktīvas (ES) 2015/2366 33. panta 1. punktā, vajadzētu būt kompetentajai iestādei, kas izraudzīta saskaņā ar Direktīvas (ES) 2015/2366 22. pantu.

(38) Tā kā lielākām finanšu vienībām varētu būt vairāk resursu un tās var 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 nozīmē. Šādām vienībām ir lielākas iespējas izveidot īpašas vadības funkcijas, lai uzraudzītu vienošanās ar trešām personām, kas sniedz IKT pakalpojumus, vai pārvarētu krīzi, organizētu IKT riska pārvaldību atbilstīgi trīs aizsardzības līniju modelim vai izveidotu iekšēju riska pārvaldības un kontroles modeli, un iesniegt iekšējai revīzijai savu IKT riska pārvaldības sistēmu.

(39) Dažas finanšu vienības gūst labumu no izņēmumiem vai arī tām piemēro ļoti atvieglotu tiesisko regulējumu saskaņā ar attiecīgajiem konkrētai nozarei piemērojamajiem Savienības tiesību aktiem. Šādas finanšu sabiedrības ietver alternatīvo ieguldījumu fondu pārvaldniekus, kas minēti Eiropas Parlamenta un Padomes Direktīvas 2011/61/ES ([16]) 3. panta 2. punktā, apdrošināšanas un pārapdrošināšanas sabiedrības, kas minētas Eiropas Parlamenta un Padomes Direktīvas 2009/138/EK ([17]) 4. pantā, un arodpensijas kapitāla uzkrāšanas institūcijas, kas pārvalda pensiju shēmas,

([14]) 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.).

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

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

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

kurās kopā nav vairāk par 15 dalībniekiem. Ņemot vērā minētos izņēmumus, nebūtu samērīgi iekļaut šādas finanšu vienības šīs regulas darbības jomā. Turklāt šajā regulā ir atzīta apdrošināšanas starpniecības tirgus struktūras specifika, tāpēc šī regula nebūtu jāpiemēro apdrošināšanas starpniekiem, pārapdrošināšanas starpniekiem un apdrošināšanas papildpakalpojuma starpniekiem, kas kvalificējami kā mikrouzņēmumi vai kā mazie vai vidējie uzņēmumi.

(40) Ņemot vērā, ka Direktīvas 2013/36/ES 2. panta 5. punkta 4.–23. apakšpunktā minētās vienības ir izslēgtas no minētās direktīvas darbības jomas, dalībvalstīm tādējādi būtu jāspēj izvēlēties atbrīvot no šīs regulas piemērošanas šādas vienības, kas atrodas to attiecīgajās teritorijās.

(41) Tāpat, lai šo regulu saskaņotu ar Eiropas Parlamenta un Padomes Direktīvas 2014/65/ES ([18]) darbības jomu, ir lietderīgi no šīs regulas darbības jomas izslēgt arī fiziskas un juridiskas personas, kas norādītas minētās direktīvas 2. un 3. pantā un kurām ir ļauts sniegt ieguldījumu pakalpojumus bez pienākuma saņemt atļauju saskaņā ar Direktīvu 2014/65/ES. Tomēr ar Direktīvas 2014/65/ES 2. pantu no minētās direktīvas darbības jomas ir izslēgtas arī vienības, kuras šīs regulas nolūkos ir uzskatāmas par finanšu vienībām, piemēram, centrālie vērtspapīru depozitāriji, kolektīvo ieguldījumu uzņēmumi vai apdrošināšanas un pārapdrošināšanas uzņēmumi. Personu un vienību, kas norādītas minētās direktīvas 2. un 3. pantā, izslēgšana no šīs regulas darbības jomas nebūtu jāattiecina uz minētajiem centrālajiem vērtspapīru depozitārijiem, kolektīvo ieguldījumu uzņēmumiem vai apdrošināšanas un pārapdrošināšanas uzņēmumiem.

(42) Saskaņā ar konkrētai nozarei piemērojamiem Savienības tiesību aktiem dažām finanšu vienībām piemēro mazāk stingras prasības vai izņēmumus tādu iemeslu dēļ, kas saistīti ar to lielumu vai sniegtajiem pakalpojumiem. Minētajā finanšu vienību kategorijā ietilpst nelielas un savstarpēji nesaistītas ieguldījumu brokeru sabiedrības, nelielas arodpensijas kapitāla uzkrāšanas institūcijas, kuras attiecīgā dalībvalsts var izslēgt no Direktīvas (ES) 2016/2341 darbības jomas saskaņā ar minētās direktīvas 5. pantā paredzētajiem nosacījumiem un kuras pārvalda pensiju shēmas, kurās kopā nav vairāk par 100 dalībniekiem, kā arī iestādes, kurām piemēro izņēmumu saskaņā ar Direktīvu 2013/36/ES. Tāpēc saskaņā ar proporcionalitātes principu un lai saglabātu konkrētai nozarei piemērojamo Savienības tiesību aktu garu, ir arī lietderīgi minētajām finanšu vienībām piemērot vienkāršotu IKT riska pārvaldības sistēmu saskaņā ar šo regulu. Regulatīvajiem tehniskajiem standartiem, kas jāizstrādā EUI, nebūtu jāizmaina minētajām finanšu vienībām piemērojamās IKT riska pārvaldības sistēmas samērīgums. Turklāt saskaņā ar proporcionalitātes principu ir lietderīgi arī maksājumu iestādēm, kas minētas Direktīvas (ES) 2015/2366 32. panta 1. punktā, un elektroniskās naudas iestādēm, kas minētas Direktīvas 2009/110/EK 9. pantā un kam piemēro izņēmumu saskaņā ar valsts tiesību aktiem, ar kuriem transponē minētos Savienības tiesību aktus, piemērot vienkāršotu IKT riska pārvaldības sistēmu saskaņā ar šo regulu, savukārt maksājumu iestādēm un elektroniskās naudas iestādēm, kurām nepiemēro izņēmumu saskaņā ar to attiecīgajiem valsts tiesību aktiem, ar kuriem transponē Savienības nozaru tiesību aktus, būtu jāievēro šajā regulā noteiktais vispārējais regulējums.

(43) Tāpat finanšu vienībām, kas kvalificējamas kā mikrouzņēmumi vai kurām piemēro vienkāršotu IKT riska pārvaldības sistēmu saskaņā ar šo regulu, nebūtu jānosaka par pienākumu izveidot funkciju, ar kuru uzrauga ar trešām personām, kas sniedz IKT pakalpojumus, noslēgtos līgumus par IKT pakalpojumu izmantošanu; vai iecelt augstākās vadības locekli, kas atbild par to, lai tiktu uzraudzīta pakļautība riskam un attiecīgie dokumenti; uzticēt kontroles funkcijai atbildību par IKT riska pārvaldību un pārraudzību un, lai nepieļautu interešu konfliktus, nodrošināt, ka šādai kontroles funkcijai ir pienācīgs neatkarības līmenis; vismaz reizi gadā dokumentēt un pārskatīt IKT riska pārvaldības sistēmu; regulāri veikt IKT riska pārvaldības sistēmas iekšējo revīziju; veikt padziļinātus novērtējumus pēc būtiskām izmaiņām to tīklu un informācijas sistēmu infrastruktūrā un procesos; regulāri veikt mantoto IKT sistēmu riska analīzi; neatkarīgās iekšējās revīzijās veikt IKT reaģēšanas un seku novēršanas plānu īstenošanas pārskatīšanu; izveidot krīzes pārvaldības funkciju, paplašināt darbības nepārtrauktības un reaģēšanas un seku novēršanas plānu testēšanu, lai aptvertu pārslēgšanās scenārijus starp primāro IKT infrastruktūru un rezerves mehānismiem; pēc kompetento iestāžu pieprasījuma ziņot tām aplēses par gada kopējām izmaksām un zaudējumiem, ko radījuši būtiski ar IKT saistīti incidenti, uzturēt rezerves IKT jaudu; paziņot valstu kompetentajām iestādēm par izmaiņām, kas ieviestas pēc tādu incidentu pārskatīšanas, kuri saistīti ar IKT; pastāvīgi uzraudzīt

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

attiecīgo tehnoloģisko attīstību, izveidot visaptverošu digitālās darbības noturības testēšanas programmu kā šajā regulā minētās IKT riska pārvaldības sistēmas neatņemamu daļu vai pieņemt un regulāri pārskatīt ar trešo personu saistītā IKT riska stratēģiju. Turklāt mikrouzņēmumiem būtu jāuzliek par pienākumu novērtēt vajadzību uzturēt šādu rezerves IKT jaudu, pamatojoties tikai uz to riska profilu. Mikrouzņēmumiem būtu jāpiemēro elastīgāks režīms attiecībā uz digitālās darbības noturības testēšanas programmām. Apsverot veicamās testēšanas veidu un biežumu, tiem būtu pienācīgi jālīdzsvaro mērķis saglabāt augstu digitālās darbības noturību, pieejamie resursi un to vispārējais riska profils. Mikrouzņēmumi un finanšu vienības, kurām piemēro vienkāršotu IKT riska pārvaldības sistēmu saskaņā ar šo regulu, būtu jāatbrīvo no prasības veikt IKT rīku, sistēmu un procesu padziļinātu testēšanu, balstoties uz draudu vadītu ielaušanās testēšanu (DVIT), jo tikai tādām finanšu vienībām, kas atbilst šajā regulā izklāstītajiem kritērijiem, vajadzētu būt pienākumam veikt šādu testēšanu. Ņemot vērā mikrouzņēmumu ierobežotās spējas, tiem būtu jāspēj vienoties ar trešām personām, kas sniedz IKT pakalpojumus, ka piekļuves, pārbaudes un revīzijas veikšanas tiesības tiek deleģētas neatkarīgai trešai personai, kuru iecēlusi trešā persona, kas sniedz IKT pakalpojumus, ar noteikumu, ka finanšu vienība no attiecīgās neatkarīgās trešās personas var jebkurā brīdī pieprasīt visu attiecīgo informāciju un garantiju par izpildes rezultātu, ko nodrošina trešā persona, kas sniedz IKT pakalpojumus.

(44) Tā kā draudu vadīti ielaušanās testi būtu obligāti jāveic tikai tām finanšu vienībām, kas identificētas padziļinātās digitālās darbības noturības testēšanas mērķiem, ar šādu testu veikšanu saistītie administratīvie procesi un finansiālās izmaksas būtu jāsedz nelielam skaitam finanšu vienību.

(45) Lai nodrošinātu pilnīgu saskaņotību un kopējo vienveidību starp finanšu vienību uzņēmējdarbības stratēģijām, no vienas puses, un IKT riska pārvaldības veikšanu, no otras puses, finanšu vienību vadības struktūrām būtu jāsaglabā nozīmīga un aktīva loma IKT riska pārvaldības sistēmas un kopējās digitālās darbības noturības stratēģijas vadībā un pielāgošanā. Vadības struktūru pieejai vajadzētu būt ne vien vērstai uz to, kā nodrošināt IKT sistēmu noturību, bet arī būtu jāaptver cilvēki un procesi, izmantojot rīcībpolitikas pasākumu kopumu, kas katrā korporatīvās vadības līmenī un attiecībā uz visu personālu sekmē labu izpratni par kiberriskiem un apņemšanos visos līmeņos ievērot stingru kiberhigiēnu. Vadības struktūras galīgajai atbildībai par finanšu vienības IKT riska pārvaldību vajadzētu būt šādas visaptverošas pieejas vispārējam principam, kas tālāk izpaužas kā vadības struktūras pastāvīga iesaiste IKT riska pārvaldības uzraudzības kontrolē.

(46) Turklāt princips, ka vadības struktūra ir pilnībā un galīgi atbildīga par finanšu vienības IKT riska pārvaldību, saskan ar vajadzību nodrošināt tādu ar IKT saistītu ieguldījumu līmeni un kopējo finanšu vienības budžetu, kas ļautu finanšu vienībai sasniegt augstu digitālās darbības noturības līmeni.

(47) Pamatojoties uz starptautisko, nacionālo un nozares attiecīgo paraugpraksi, pamatnostādnēm, ieteikumiem un pieejām kiberriska pārvaldībai, šī regula veicina tādu principu kopumu, kas sekmē IKT riska pārvaldības vispārējo strukturēšanu. Tādējādi, ja galvenās spējas, ko ievieš finanšu vienības, risina šajā regulā noteiktās dažādās funkcijas, kas ietvertas IKT riska pārvaldībā (identifikācija, aizsardzība un profilakse, atklāšana, reaģēšana un seku novēršana, mācīšanās un attīstība, saziņa), finanšu vienībām arī turpmāk vajadzētu būt iespējai brīvi izmantot dažādi formulētus vai citā kategorijā iekļautus IKT riska pārvaldības modeļus.

(48) Lai neatpaliktu no strauji mainīgās kiberdraudu vides, finanšu vienībām būtu jāuztur atjauninātas IKT sistēmas, kas ir uzticamas un spēj ne tikai garantēt to pakalpojumiem nepieciešamo datu apstrādi, bet arī nodrošināt pietiekamu tehnoloģisko noturību, lai ļautu tām pienācīgi veikt papildu apstrādi, kas vajadzīga saspringtu tirgus apstākļu vai citas nelabvēlīgas situācijas dēļ.

(49) 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 seku novēršanas darbībām saskaņā ar to rezerves kopiju veidošanas politiku. Tomēr šāda darbību atsākšana nedrīkstētu nekādā veidā apdraudēt tīklu un informācijas sistēmu integritāti un drošību vai datu pieejamību, autentiskumu, integritāti vai konfidencialitāti.

(50) Lai gan šī regula ļauj finanšu vienībām elastīgi konstatēt mērķus attiecībā uz saviem atgūšanas termiņiem un atgūšana punktu un līdz ar to noteikt šādus mērķus, pilnībā ņemot vērā attiecīgo funkciju būtību un kritisko svarīgumu, kā arī jebkādas specifiskās uzņēmējdarbības vajadzības, jebkurā gadījumā tajā būtu jāuzliek pienākums šīm vienībām mērķu noteikšanas procesā veikt novērtējumu par iespējamo kopējo ietekmi uz tirgus efektivitāti.

(51) Kiberuzbrukumu īstenotāji parasti cenšas gūt finansiālus ieguvumus tieši līdzekļu izcelsmes vietā, tādējādi radot būtiskas sekas finanšu vienībām. Lai novērstu to, ka IKT sistēmas zaudē integritāti vai kļūst nepieejamas, un tādējādi novērstu datu pārkāpumus un kaitējumu fiziskajai IKT infrastruktūrai, būtu ievērojami jāuzlabo un jāracionalizē finanšu vienību ziņošana par būtiskiem ar IKT saistītiem incidentiem. Ar IKT saistītu incidentu paziņošana būtu jāsaskaņo, nosakot prasību visām finanšu vienībām ziņot tieši to attiecīgajām kompetentajām iestādēm. Ja finanšu vienību uzrauga vairāk nekā viena valsts kompetentā iestāde, dalībvalstīm būtu jāizraugās viena kompetentā iestāde, kurai adresē šādus ziņojumus. Kredītiestādēm, kas saskaņā ar Padomes Regulas (ES) Nr. 1024/2013 ([19]) 6. panta 4. punktu klasificētas kā nozīmīgas, būtu jāiesniedz minētie ziņojumi valsts kompetentajām iestādēm, kurām pēc tam attiecīgais ziņojums būtu jānosūta Eiropas Centrālajai bankai (ECB).

(52) Tiešai ziņošanai būtu jāļauj finanšu uzraudzības iestādēm nekavējoties piekļūt informācijai par būtiskiem ar IKT saistītiem incidentiem. Savukārt finanšu uzraudzības iestādēm par būtiskiem ar IKT saistītiem incidentiem būtu jāinformē publiskās nefinanšu iestādes (piemēram, kompetentās iestādes un vienotie kontaktpunkti saskaņā ar Direktīvu (ES) 2022/2555, valsts datu aizsardzības iestādes un tiesībaizsardzības iestādes par būtiskiem ar IKT saistītiem krimināla rakstura incidentiem), lai uzlabotu šādu iestāžu informētību par šādiem incidentiem un *CSIRT* gadījumā sekmētu ātru palīdzību, ko attiecīgā gadījumā var sniegt finanšu vienībām. Turklāt dalībvalstīm būtu jāspēj noteikt, ka finanšu vienībām pašām būtu šāda informācija jāsniedz publiskām iestādēm, kas nav saistītas ar finanšu pakalpojumu jomu. Minētajai informācijas nodošanai būtu jādod iespēja finanšu vienībām ātri iegūt attiecīgo tehnisko informāciju, konsultācijas par tiesiskās aizsardzības līdzekļiem un informāciju par turpmākiem šādu iestāžu veiktiem pasākumiem. Informācija par būtiskiem ar IKT saistītiem incidentiem būtu jāsniedz abpusēji: finanšu uzraudzības iestādēm būtu jāsniedz finanšu vienībai visa nepieciešamā atgriezeniskā saite vai norādījumi, savukārt EUI būtu jādalās ar anonimizētiem datiem par kiberdraudiem un ievainojamību, kas saistīti ar incidentu, lai palīdzētu veidot kolektīvo aizsardzību plašākā nozīmē.

(53) Lai gan visām finanšu vienībām būtu jāuzliek par pienākumu ziņot par incidentiem, nav paredzēts, ka šī prasība vienādi skars tās visas. Faktiski attiecīgās būtiskuma robežvērtības, kā arī paziņošanas termiņi būtu pienācīgi jāpielāgo, ņemot vērā deleģētos aktus, kuru pamatā ir regulatīvie tehniskie standarti, kas jāizstrādā EUI, lai aptvertu tikai būtiskus ar IKT saistītus incidentus. Turklāt, nosakot termiņus saistībā ar ziņošanas pienākumu, būtu jāņem vērā finanšu vienību īpatnības.

(54) Šajā regulā būtu jānosaka prasība kredītiestādēm, maksājumu iestādēm, konta informācijas pakalpojumu sniedzējiem un elektroniskās naudas iestādēm ziņot par visiem ar maksājumiem saistītajiem darbības vai drošības incidentiem – par kuriem iepriekš bija jāziņo saskaņā ar Direktīvu (ES) 2015/2366 – neatkarīgi no tā, vai incidents ir vai nav saistīts ar IKT.

([19]) 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.).

(55) EUI būtu jāuztic uzdevums izvērtēt iespējamību un nosacījumus ar IKT saistītas incidentu paziņošanas iespējamai centralizācijai Savienības līmenī. Šāda centralizēšana varētu ietvert vienotu ES centrmezglu ziņošanai par būtiskiem ar IKT saistītiem incidentiem, kas vai nu tieši saņemtu attiecīgos ziņojumus un automātiski informētu valstu kompetentās iestādes, vai centralizētu attiecīgos valstu kompetento iestāžu pārsūtītos ziņojumus un tādējādi pildītu koordinācijas funkciju. EUI būtu jāuztic uzdevums, apspriežoties ar ECB un *ENISA*, izstrādāt kopīgu ziņojumu, kurā būtu izvērtēta šāda vienota ES centrmezgla izveides iespējamība.

(56) Lai panāktu augstu digitālās darbības noturības līmeni, kā arī ievērojot attiecīgos starptautiskos standartus (piemēram, G7 draudu vadītas ielaušanās testēšanas pamatelementus) un izmantojot tādas Savienībā piemērojamas sistēmas kā *TIBER-EU*, finanšu vienībām būtu regulāri jātestē savu IKT sistēmu un personāla, kam ir ar IKT saistīti pienākumi, preventīvo, atklāšanas, reaģēšanas un seku novēršanas spēju efektivitāte, lai atklātu un risinātu potenciālo IKT ievainojamību. Lai atspoguļotu dažādo finanšu apakšnozaru starpā un to iekšienē pastāvošās atšķirības saistībā ar finanšu vienību sagatavotību kiberdrošības jomā, testēšanā būtu jāietver plašs rīku un darbību klāsts, sākot no pamatprasību novērtēšanas (piemēram, ievainojamības 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, izmantojot DVIT. Šāda padziļināta testēšana būtu jāpieprasa tikai tām finanšu vienībām, kuru sagatavotība no IKT viedokļa ir pietiekama, lai to varētu pamatoti veikt. Tādēļ digitālās darbības noturības testēšanai, kas prasīta šajā regulā, attiecībā uz tām finanšu vienībām, kas atbilst šajā regulā izklāstītajiem kritērijiem (piemēram, lielām, sistēmiskām un IKT ziņā nobriedušām kredītiestādēm, biržām, centrālajiem vērtspapīru depozitārijiem un centrālajiem darījumu partneriem) būtu jābūt prasīgākai nekā attiecībā uz citām finanšu vienībām. Vienlaikus digitālās darbības noturības testēšanai, izmantojot DVIT, būtu jābūt lielākai attiecībā uz finanšu vienībām, kuras darbojas finanšu pamatpakalpojumu apakšnozarēs un kam ir sistēmiska loma (piemēram, maksājumi, banku darbība un tīrvērte un norēķini), bet mazākai – attiecībā uz citām apakšnozarēm (piemēram, aktīvu pārvaldītāji un kredītreitingu aģentūras).

(57) Finanšu vienībām, kas ir iesaistītas pārrobežu darbībās un izmanto iedibinājumbrīvību vai brīvību 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 finanšu grupa darbojas Savienībā, tādējādi pieļaujot, ka šādām pārrobežu finanšu grupām ar IKT saistītas testēšanas izmaksas rodas tikai vienā jurisdikcijā.

(58) Lai izmantotu pieredzi, ko dažas kompetentās iestādes jau guvušas, jo īpaši saistībā ar *TIBER-EU* sistēmas īstenošanu, šajā regulā būtu jāļauj dalībvalstīm izraudzīties vienu publisku iestādi par atbildīgo finanšu nozarē valsts līmenī attiecībā uz visiem DVIT jautājumiem vai, ja šāda izraudzīšana nav veikta, kompetentajām iestādēm deleģēt ar DVIT saistītu uzdevumu veikšanu citai valsts finanšu kompetentajai iestādei.

(59) Ņemot vērā to, ka šajā regulā nav noteikta prasība finanšu vienībām ietvert visas kritiski svarīgās vai svarīgās funkcijas vienā draudu vadītā ielaušanās testā, finanšu vienībām vajadzētu būt iespējai brīvi noteikt, kuras un cik daudz kritiski svarīgu vai svarīgu funkciju būtu iekļaujamas šāda testa tvērumā.

(60) Apvienota testēšana šīs regulas nozīmē – kurā DVIT ir iesaistītas vairākas finanšu vienības un attiecībā uz kuru trešās personas, kas sniedz IKT pakalpojumus, var tieši noslēgt līgumiskas vienošanās ar ārēju testētāju – būtu jāatļauj tikai tad, ja ir pamatoti sagaidāms, ka tiks negatīvi ietekmēta to pakalpojumu kvalitāte vai drošība, kurus trešā persona, kas sniedz IKT pakalpojumus, sniedz klientiem, kas ir vienības, kuras neietilpst šīs regulas darbības jomā, vai ar šādiem pakalpojumiem saistītu datu konfidencialitāte. Apvienotai testēšanai būtu jāpiemēro arī aizsardzības pasākumi (vienas izraudzītas finanšu vienības sniegtas norādes, iesaistīto finanšu vienību skaita kalibrēšana), lai nodrošinātu to iesaistīto finanšu vienību stingru testēšanu, kuras atbilst DVIT mērķiem saskaņā ar šo regulu.

(61) Lai izmantotu korporatīvā līmenī pieejamos iekšējos resursus, šajā regulā būtu jāatļauj DVIT veikšanas nolūkā izmantot iekšējos testētājus, ar noteikumu, ka ir saņemts uzraudzības iestādes apstiprinājums, nav interešu konfliktu un ir periodiski mainīta iekšējo testētāju un ārējo testētāju (katrs trešais tests) izmantošana, vienlaikus arī pieprasot, lai draudu izlūkdatu sniedzējs DVIT vienmēr būtu ārējs un ar finanšu vienību nesaistīts. Atbildība par DVIT veikšanu būtu pilnībā jāuzņemas finanšu vienībai. Iestāžu sniegtajiem apliecinājumiem vajadzētu būt sniegtiem tikai savstarpējas atzīšanas nolūkā, un tiem nebūtu jāliedz veikt turpmākus pasākumus, kas vajadzīgi, lai novērstu IKT risku, kuram finanšu vienība ir pakļauta, kā arī tos nebūtu jāuzskata par finanšu vienības IKT riska pārvaldības un mazināšanas spēju uzraudzības apstiprinājumu.

(62) Lai nodrošinātu ar trešo personu saistītā IKT riska stabilu uzraudzību finanšu nozarē, ir nepieciešams paredzēt uz principiem balstītu noteikumu kopumu, kas palīdzētu finanšu vienībām, kad tās veic tāda riska uzraudzību, kas rodas saistībā ar funkciju nodošanu ārpakalpojumā trešām personām, kas sniedz IKT pakalpojumus, jo īpaši IKT pakalpojumus, kas atbalsta kritiski svarīgas vai svarīgas funkcijas, kā arī vispārīgāk – saistībā ar visu veidu atkarību no trešām personām, kas sniedz IKT pakalpojumu.

(63) Lai risinātu IKT riska dažādo avotu sarežģītību, vienlaikus ņemot vērā tādu tehnoloģisko risinājumu sniedzēju lielo skaitu un daudzveidību, kas ļauj netraucēti sniegt finanšu pakalpojumus, šai regulai būtu jāattiecas uz plašu to trešo personu loku, kas sniedz IKT pakalpojumus, tostarp mākoņdatošanas pakalpojumu, programmatūras, datu analītikas pakalpojumu un datu centru pakalpojumu sniedzējiem. Ņemot vērā, ka finanšu vienībām būtu efektīvi un saskaņoti jāapzina un jāpārvalda visu veidu riski, tostarp saistībā ar IKT pakalpojumiem, kuri iepirkti finanšu grupā, būtu arī jāprecizē, ka uzņēmumi, kas ietilpst finanšu grupā un sniedz IKT pakalpojumus galvenokārt savam mātesuzņēmumam vai to mātesuzņēmuma meitasuzņēmumiem vai filiālēm, kā arī finanšu vienības, kas sniedz IKT pakalpojumus citām finanšu vienībām, saskaņā ar šo regulu arī būtu jāuzskata par trešo personu, kas sniedz IKT pakalpojumus. Visbeidzot, ņemot vērā, ka mainīgais maksājumu pakalpojumu tirgus kļūst arvien atkarīgāks no sarežģītiem tehniskiem risinājumiem, un ņemot vērā jaunos maksājumu pakalpojumu veidus un ar maksājumiem saistītus risinājumus, maksājumu pakalpojumu ekosistēmas dalībnieki, kuri veic maksājumu apstrādes darbības vai pārvalda maksājumu infrastruktūru, saskaņā ar šo regulu arī būtu jāuzskata par trešām personām, kas sniedz IKT pakalpojumus, izņemot centrālās bankas, kad tiek izmantotas maksājumu vai vērtspapīru norēķinu sistēmas, un publiskās iestādes, kad tiek sniegti ar IKT saistīti pakalpojumi valsts funkciju pildīšanas kontekstā.

(64) Finanšu vienībai vajadzētu nepārtraukti būt pilnībā atbildīgai par šajā regulā tai noteikto pienākumu izpildi. Finanšu vienībām būtu jāpiemēro samērīga pieeja tādu risku uzraudzībai, kas rodas trešām personām, kas sniedz IKT pakalpojumus, pienācīgi ņemot vērā savas ar IKT saistītās atkarības veidu, 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.

(65) Šādā uzraudzībā būtu jāievēro stratēģiska pieeja ar trešo personu saistītajam IKT riskam, kas tiek formalizēta, finanšu vienības vadības struktūrai pieņemot īpašu ar trešo personu saistītā IKT riska stratēģiju, kas balstās visu veidu 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 darbu saistībā ar pārraudzības sistēmu, kas izveidota ar šo regulu, visām finanšu vienībām būtu jāuzliek par pienākumu uzturēt informācijas reģistru attiecībā uz katru līgumisko vienošanos par izmantotajiem IKT pakalpojumiem, ko sniedz trešās personas, kas sniedz IKT pakalpojumus. Finanšu uzraudzības iestādēm būtu jāspēj pieprasīt pilnu reģistru vai konkrētas tā daļas un tādējādi saņemt būtisku informāciju, lai gūtu plašāku izpratni par finanšu vienību atkarību no IKT.

(66) Padziļinātai analīzei pirms līguma noslēgšanas vajadzētu būt līgumiskas vienošanās oficiālas noslēgšanas pamatā un jānotiek pirms tās, jo īpaši pievēršoties tādiem elementiem kā paredzētā IKT līguma atbalstīto pakalpojumu kritiskums vai svarīgums, nepieciešamie uzraudzības iestāžu apstiprinājumi vai citi nosacījumi, iespējamais ar to saistītais koncentrācijas risks, kā arī pienācīgas rūpības piemērošana trešo personu, kas sniedz IKT pakalpojumus, atlases un novērtēšanas procesā un iespējamo interešu konfliktu novērtēšana. Attiecībā uz līgumisku vienošanos par kritiski svarīgām vai svarīgām funkcijām finanšu vienībām būtu jāņem vērā tas, ka trešās personas, kas sniedz IKT pakalpojumus, izmanto visjaunākos un visaugstākos informācijas drošības standartus. Līgumiskas vienošanās izbeigšanu varētu izraisīt vismaz vairāki apstākļi, kas liecina par nepilnībām trešās personas, kas sniedz IKT

pakalpojumus, līmenī, jo īpaši būtiski tiesību aktu vai līguma noteikumu pārkāpumi, apstākļi, kas atklāj iespējamas izmaiņas to funkciju izpildē, ko paredz līgumiskās vienošanās, pierādījumi par trešās personas, kas sniedz IKT pakalpojumus, nepilnībām vispārējā IKT riska pārvaldībā vai apstākļi, kas liecina par attiecīgās kompetentās iestādes nespēju efektīvi uzraudzīt finanšu vienību.

(67) Lai risinātu ar trešo personu saistītā IKT koncentrācijas riska sistēmisko ietekmi, šajā regulā tiek sekmēts līdzsvarots risinājums, pieņemot elastīgu un pakāpenisku pieeju šādam koncentrācijas riskam, jo jebkādu neelastīgu robežvērtību vai stingru ierobežojumu noteikšana varētu kavēt uzņēmējdarbības veikšanu un ierobežot līgumslēgšanas brīvību. Finanšu vienībām būtu rūpīgi jāizvērtē savas paredzētās līgumiskās vienošanās, lai noteiktu šāda riska rašanās iespējamību, tostarp veicot padziļinātu analīzi par apakšuzņēmuma līgumiem, jo īpaši, ja tie noslēgti ar trešā valstī iedibinātām trešām personām, kas sniedz IKT pakalpojumus. Šajā posmā un nolūkā panākt taisnīgu līdzsvaru starp līgumu slēgšanas brīvības saglabāšanu un finanšu stabilitātes garantēšanu nav lietderīgi noteikt stingras robežvērtības un ierobežojumus pakļautībai ar trešo personu saistītam IKT riskam. Pārraudzības sistēmas kontekstā galvenajam pārraugam, kas iecelts, ievērojot šo regulu, attiecībā uz kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, būtu īpaša uzmanība jāpievērš tam, lai pilnībā aptvertu savstarpējo atkarību apjomu, jāatklāj konkrēti gadījumi, kad kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, augsta koncentrācija Savienībā varētu radīt spiedienu uz Savienības finanšu sistēmas stabilitāti un integritāti, un jāuztur dialogs ar kritiski svarīgajām trešām personām, kas sniedz IKT pakalpojumus, ja šāds konkrēts risks ir identificēts.

(68) Lai regulāri izvērtētu un uzraudzītu trešās personas, kas sniedz IKT pakalpojumus, spēju droši sniegt pakalpojumus finanšu vienībai, nelabvēlīgi neietekmējot finanšu vienības digitālās darbības noturību, būtu jāsaskaņo vairāki galvenie līgumiskie elementi ar trešām personām, kas sniedz IKT pakalpojumus. Šādai saskaņošanai būtu jāaptver minimālās jomas, kas ir būtiskas, lai ļautu finanšu vienībai pilnībā uzraudzīt riskus, ko varētu radīt trešā persona, kas sniedz IKT pakalpojumus, ņemot vērā finanšu vienības vajadzību nodrošināt savu digitālo noturību, jo tā ir ļoti atkarīga no saņemto IKT pakalpojumu stabilitātes, funkcionalitātes, pieejamības un drošības.

(69) Pārskatot līgumiskās vienošanās, lai panāktu saskaņotību ar šīs regulas prasībām, finanšu vienībām un trešām personām, kas sniedz IKT pakalpojumus, būtu jānodrošina, ka tajās ir iekļauti galvenie šajā regulā paredzētie līgumu noteikumi.

(70) Šajā regulā sniegtā jēdziena "kritiski svarīgas vai svarīgas funkcijas" definīcija ietver "kritiski svarīgas funkcijas", kā tās definētas Eiropas Parlamenta un Padomes Direktīvas 2014/59/ES ([20]) 2. panta 1. punkta 35) apakšpunktā. Tāpēc funkcijas, ko uzskata par kritiski svarīgām, ievērojot Direktīvu 2014/59/ES, ir iekļautas kritiski svarīgo funkciju definīcijā šīs regulas nozīmē.

(71) Neatkarīgi no IKT pakalpojumu atbalstītās funkcijas kritiskuma vai svarīguma ar līgumisku vienošanos jo īpaši būtu jānosaka funkciju un pakalpojumu pilnīgs apraksts, šādu funkciju sniegšanas un datu apstrādes vieta, kā arī jānorāda pakalpojumu līmeņa apraksti. Citi būtiski elementi, lai ļautu finanšu vienībai uzraudzīt ar trešo personu saistīto IKT risku, ir: līguma noteikumi, kuros precizēts, kā trešā persona, kas sniedz IKT pakalpojumus, nodrošina personas datu piekļūstamību, pieejamību, integritāti, drošību un aizsardzību, noteikumi, ar ko tiek garantēta piekļuve datiem un to atgūšana un atgriešana trešās personas, kas sniedz IKT pakalpojumus, maksātnespējas, noregulējuma vai uzņēmējdarbības izbeigšanas gadījumā, kā arī noteikumi, kuros paredzēts, ka trešās personas, kas sniedz IKT pakalpojumus, nodrošina palīdzību ar sniegto pakalpojumu saistītu IKT incidentu gadījumā bez papildu izmaksām vai par iepriekš noteiktu maksu; noteikumi, kuros paredzēts trešās personas, kas sniedz IKT pakalpojumus, pienākums pilnībā sadarboties ar finanšu vienības kompetentajām iestādēm un noregulējuma iestādēm; un noteikumi par izbeigšanas tiesībām un ar tām saistītajiem minimālajiem paziņošanas termiņiem attiecībā uz

([20]) Eiropas Parlamenta un Padomes Direktīva 2014/59/ES (2014. gada 15. maijs), ar ko izveido kredītiestāžu un ieguldījumu brokeru sabiedrību atveseļošanas un noregulējuma režīmu un groza Padomes Direktīvu 82/891/EEK un Eiropas Parlamenta un Padomes Direktīvas 2001/24/EK, 2002/47/EK, 2004/25/EK, 2005/56/EK, 2007/36/EK, 2011/35/ES, 2012/30/ES un 2013/36/ES, un Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1093/2010 un (ES) Nr. 648/2012 (OV L 173, 12.6.2014., 190. lpp.).

līgumiskās vienošanās izbeigšanu atbilstoši tam, kā to sagaida kompetentās iestādes un noregulējuma iestādes.

(72) Papildus šādiem līguma noteikumiem un lai nodrošinātu, ka finanšu vienības saglabā pilnīgu kontroli pār visu notikumu attīstību trešo personu līmenī, kas var mazināt to IKT drošību, līgumos par tādu IKT pakalpojumu sniegšanu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, būtu jāparedz arī šādi elementi: pilnīgu pakalpojumu līmeņa aprakstu specifikācija ar precīziem kvantitatīviem un kvalitatīviem darbības mērķiem, lai bez liekas kavēšanās varētu veikt atbilstīgus koriģējošus pasākumus, ja netiek ievēroti saskaņotie pakalpojumu līmeņi; trešās personas, kas sniedz IKT pakalpojumus, attiecīgie saistošie paziņošanas termiņi un ziņošanas pienākumi tādu notikumu gadījumā, kas var būtiski ietekmēt trešās personas, kas sniedz IKT pakalpojumus, spēju efektīvi sniegt savus attiecīgos IKT pakalpojumus; prasība trešai personai, kas sniedz IKT pakalpojumus, īstenot un pārbaudīt uzņēmējdarbības ārkārtas rīcības plānus un ieviest IKT drošības pasākumus, rīkus un politiku, kas ļauj droši sniegt pakalpojumus, kā arī piedalīties un pilnībā sadarboties DVIT, ko veic finanšu vienība.

(73) Līgumos par tādu IKT pakalpojumu sniegšanu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, vajadzētu ietvert arī noteikumus, kas ļauj īstenot finanšu vienības vai ieceltas trešās personas piekļuves, pārbaudes un revīzijas tiesības un tiesības izgatavot kopijas kā svarīgu rīku finanšu vienības veiktās trešās personas, kas sniedz IKT pakalpojumus, darbības rezultātu pastāvīgās uzraudzības procesā, ko papildina pakalpojumu sniedzēja pilnīga sadarbība pārbaužu laikā. Arī finanšu vienības kompetentajai iestādei vajadzētu būt tiesībām ar iepriekšēju paziņojumu pārbaudīt trešo personu, kas sniedz IKT pakalpojumus, un veikt tā revīziju, nodrošinot konfidenciālas informācijas aizsardzību.

(74) Ar šādu līgumisku vienošanos būtu arī jāparedz skaidri noteiktas atsevišķas atkāpšanās stratēģijas, kas jo īpaši ļauj noteikt obligātus pārejas periodus, kuros trešām personām, kas sniedz IKT pakalpojumus, būtu jāturpina nodrošināt attiecīgos pakalpojumus ar mērķi mazināt traucējumu risku finanšu vienības līmenī, vai jāļauj finanšu vienībai efektīvi pāriet pie citas trešās personas izmantošanas, kas sniedz IKT pakalpojumus, vai arī pāriet uz iekšējiem risinājumiem atbilstīgi sniegtā IKT pakalpojuma sarežģītībai. Turklāt finanšu vienībām, uz kurām attiecas Direktīvas 2014/59/ES darbības joma, būtu jānodrošina, ka attiecīgie līgumi par IKT pakalpojumiem ir stabili un pilnībā izpildāmi minēto finanšu vienību noregulējuma gadījumā. Tādēļ noregulējuma iestādes sagaida, ka minētās finanšu vienības nodrošinās, lai attiecīgie IKT pakalpojumu līgumi būtu noturīgi noregulējuma gadījumā. Kamēr minētās finanšu vienības turpina pildīt savas maksājumu saistības, tām cita starpā būtu jānodrošina, ka attiecīgajos IKT pakalpojumu līgumos ir ietvertas klauzulas par līguma darbības neizbeigšanu, neatcelšanu un nepārveidošanu pārstrukturēšanas vai noregulējuma gadījumā.

(75) Turklāt, brīvprātīgi izmantojot līguma standartklauzulas, kuras izstrādājušas valsts iestādes vai Savienības iestādes, jo īpaši līguma klauzulas, ko Komisija izstrādājusi attiecībā uz mākoņdatošanas pakalpojumiem, varētu nodrošināt papildu drošību finanšu vienībām un trešām personām, kas sniedz IKT pakalpojumus, uzlabojot to juridisko noteiktību attiecībā uz mākoņdatošanas pakalpojumu izmantošanu finanšu nozarē un to pilnībā saskaņojot ar Savienības finanšu pakalpojumu tiesību aktu prasībām un gaidām. Līguma standartklauzulu izstrāde 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.

(76) Lai veicinātu konverģenci un efektivitāti attiecībā uz uzraudzības pieejām, ar ko pievēršas ar trešo personu saistītajam IKT riskam finanšu nozarē, kā arī lai stiprinātu to finanšu vienību digitālās darbības noturību, kuras tādu IKT pakalpojumu sniegšanai, ar kuriem atbalsta finanšu pakalpojumus, paļaujas uz kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, un tādējādi palīdzētu saglabāt Savienības finanšu sistēmas stabilitāti un finanšu pakalpojumu iekšējā tirgus integritāti, uz kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, vajadzētu attiekties Savienības pārraudzības sistēmai. Lai gan pārraudzības sistēmas izveide ir pamatota ar pievienoto vērtību, ko sniedz rīcība Savienības līmenī, un ņemot vērā IKT pakalpojumu izmantošanas būtisko

nozīmi un specifiku finanšu pakalpojumu sniegšanā, vienlaikus būtu jāatgādina, ka šis risinājums šķiet piemērots tikai saistībā ar šo regulu, kas īpaši attiecas uz digitālās darbības noturību finanšu nozarē. Tomēr šāda pārraudzības sistēma nebūtu jāuzskata par jaunu Savienības uzraudzības modeli citās finanšu pakalpojumu un darbību jomās.

(77) Pārraudzības sistēma būtu jāpiemēro tikai kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus. Tādēļ būtu jāparedz izraudzīšanās mehānisms, lai ņemtu vērā, kādā apmērā un veidā finanšu nozare paļaujas uz šādām trešām personām, kas sniedz IKT pakalpojumus. Minētajam mehānismam būtu jāietver kvantitatīvu un kvalitatīvu kritēriju kopums, kas noteiktu svarīguma parametrus kā pamatu iekļaušanai pārraudzības sistēmā. Lai nodrošinātu minētā novērtējuma precizitāti un neatkarīgi no trešās personas, kas sniedz IKT pakalpojumus, korporatīvās struktūras, šādos kritērijos attiecībā uz trešo personu, kas sniedz IKT pakalpojumus un ir daļa no plašākas grupas, būtu jāņem vērā visa trešās personas, kas sniedz IKT pakalpojumus, grupas struktūra. No vienas puses, kritiski svarīgajām trešām personām, kas sniedz IKT pakalpojumus un kas netiek automātiski izraudzītas, piemērojot minētos kritērijus, vajadzētu būt iespējai brīvprātīgi pievienoties pārraudzības sistēmai, savukārt tās trešās personas, kas sniedz IKT pakalpojumus, uz kurām jau attiecas pārraudzības mehānisma sistēmas, kuru mērķis ir atbalstīt LESD 127. panta 2. punktā minēto Eiropas Centrālo banku sistēmas uzdevumu pildīšanu, būtu jāatbrīvo.

(78) Līdzīgi arī finanšu vienības, kas sniedz IKT pakalpojumus citām finanšu vienībām, lai gan pieder pie trešo personu, kas sniedz IKT pakalpojumus saskaņā ar šo regulu, kategorijas, būtu jāatbrīvo no pārraudzības sistēmas, jo uz tām jau attiecas uzraudzības mehānismi, kas izveidoti ar attiecīgajiem Savienības finanšu pakalpojumu tiesību aktiem. Attiecīgā gadījumā kompetentajām iestādēm saistībā ar savām uzraudzības darbībām būtu jāņem vērā IKT risks, ko finanšu vienībām rada finanšu vienības, kuras sniedz IKT pakalpojumus. Tāpat, ņemot vērā esošos riska uzraudzības mehānismus grupas līmenī, tāds pats atbrīvojums būtu jāievieš attiecībā uz trešām personām, kas sniedz IKT pakalpojumus galvenokārt savas grupas vienībām. Trešās personas, kas sniedz IKT pakalpojumus tikai vienā dalībvalstī finanšu vienībām, kuras darbojas tikai minētajā dalībvalstī, arī būtu jāatbrīvo no izraudzīšanas mehānisma to ierobežoto darbību un pārrobežu ietekmes neesamības dēļ.

(79) Finanšu pakalpojumu jomā piedzīvotā digitālā pārveide ir radījusi vēl nepieredzētu IKT pakalpojumu izmantošanas līmeni un paļaušanos uz tiem. Tā kā ir kļuvis neiedomājami sniegt finanšu pakalpojumus, neizmantojot mākoņdatošanas pakalpojumus, programmatūras risinājumus un ar datiem saistītus pakalpojumus, Savienības finanšu ekosistēma ir kļuvusi nesaraujami atkarīga no konkrētiem IKT pakalpojumiem, ko sniedz IKT pakalpojumu sniedzēji. Dažiem no minētajiem piegādātājiem, novatoriem, kas izstrādā un izmanto uz IKT balstītas tehnoloģijas, ir nozīmīga loma finanšu pakalpojumu sniegšanā, vai arī tie ir integrējušies finanšu pakalpojumu vērtības ķēdē. Tādējādi tie ir kļuvuši kritiski svarīgi Savienības finanšu sistēmas stabilitātei un integritātei. Šī plašā paļaušanās uz pakalpojumiem, ko sniedz kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, apvienojumā ar dažādu tirgus dalībnieku informācijas sistēmu savstarpējo atkarību rada tiešu un potenciāli nopietnu risku Savienības finanšu pakalpojumu sistēmai un finanšu pakalpojumu sniegšanas nepārtrauktībai, ja kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, skartu darbības traucējumi vai būtiski kiberincidenti. Kiberincidentiem ir izteikta spēja vairoties un izplatīties visā finanšu sistēmā ievērojami ātrāk nekā citiem riska veidiem, kas tiek uzraudzīti finanšu nozarē, un tie var aptvert dažādas nozares un sniegties pāri ģeogrāfiskajām robežām. Tiem ir potenciāls pāraugt sistēmiskā krīzē, kad uzticēšanās finanšu sistēmai ir mazinājusies reālās ekonomikas atbalsta funkciju traucējumu dēļ vai būtisku finansiālu zaudējumu dēļ, sasniedzot līmeni, ko finanšu sistēma nespēj izturēt vai kam nepieciešama smagu satricinājumu absorbcijas pasākumu īstenošana. Lai novērstu to, ka šādi scenāriji var piepildīties un tādējādi apdraudēt Savienības finanšu stabilitāti un integritāti, ir būtiski nodrošināt uzraudzības prakses konverģenci attiecībā uz tādu risku finanšu jomā, kurš saistīts ar trešo personu, kas sniedz IKT pakalpojumus, jo īpaši ar jauniem noteikumiem, kas ļauj Savienībai pārraudzīt kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus.

(80) Pārraudzības sistēma lielā mērā ir atkarīga no sadarbības pakāpes starp galveno pārraugu un kritiski svarīgo trešo personu, kas finanšu vienībām sniedz tādus IKT pakalpojumus, kuri ietekmē finanšu pakalpojumu sniegšanu. Sekmīga pārraudzība cita starpā ir atkarīga no galvenā pārrauga spējas efektīvi veikt uzraudzības uzdevumus un pārbaudes, lai novērtētu noteikumus, kontroli un procesus, ko izmanto kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, kā arī lai novērtētu to darbību iespējamo kumulatīvo ietekmi uz finanšu stabilitāti un finanšu sistēmas integritāti. Vienlaikus ir būtiski, lai kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, ievērotu galvenā pārrauga ieteikumus un kliedētu viņa bažas. Tā kā tādas kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, kuri ietekmē finanšu pakalpojumu sniegšanu, sadarbības trūkums, piemēram, atteikums piešķirt piekļuvi savām telpām vai iesniegt informāciju, galu galā atņemtu galvenajam pārraugam tā būtiski svarīgos rīkus, kas vajadzīgi, lai novērtētu ar trešo personu saistītu IKT risku, un varētu negatīvi ietekmēt finanšu sistēmas finanšu stabilitāti un integritāti, ir jāparedz arī samērīgs sankciju režīms.

(81) Ņemot vērā iepriekš minēto, galvenā pārrauga vajadzību piemērot soda maksājumus, lai piespiestu kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, ievērot šajā regulā noteiktos pārredzamības un ar piekļuvi saistītos pienākumus, nedrīkstētu apdraudēt grūtības, ko rada minēto soda maksājumu izpilde attiecībā uz kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus un kas iedibināti trešās valstīs. Lai nodrošinātu šādu sodu izpildāmību un ļautu ātri ieviest procedūras, ar kurām tiek nodrošinātas kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, tiesības uz aizstāvību saistībā ar izraudzīšanas mehānismu un ieteikumu sniegšanu, minētajām kritiski svarīgām trešām personām, kas finanšu vienībām sniedz IKT pakalpojumus, kuri ietekmē finanšu pakalpojumu sniegšanu, būtu jāprasa saglabāt pienācīgu uzņēmējdarbības klātbūtni Savienībā. Ņemot vērā pārraudzības būtību un salīdzināmu pasākumu trūkumu citās jurisdikcijās, nav piemērotu alternatīvu mehānismu, kas nodrošinātu šo mērķi, efektīvi sadarbojoties ar finanšu uzraudzības iestādēm trešās valstīs saistībā ar to digitālo operacionālo risku ietekmes uzraudzību, kurus rada trešās personas, kas sniedz sistēmiskus IKT pakalpojumus un kvalificējas kā kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus un kas iedibinātas trešās valstīs. Tāpēc, lai turpinātu sniegt IKT pakalpojumus finanšu vienībām Savienībā, trešai personai, kas sniedz IKT pakalpojumus un kas iedibināta trešās valstīs, un kas saskaņā ar šo regulu ir izraudzīta par kritiski svarīgu, 12 mēnešu laikā pēc šādas izraudzīšanas būtu jāveic visi nepieciešamie pasākumi, lai nodrošinātu tās nodibināšanu Savienībā, iedibinot meitasuzņēmumu, kā definēts visā Savienības *acquis*, jo īpaši Eiropas Parlamenta un Padomes Direktīvā 2013/34/ES ([21]).

(82) Prasībai izveidot meitasuzņēmumu Savienībā nebūtu jāliedz kritiski svarīgai trešai personai, kas sniedz IKT pakalpojumus, sniegt IKT pakalpojumus un saistīto tehnisko atbalstu no objektiem un infrastruktūras, kas atrodas ārpus Savienības. Ar šo regulu nenosaka datu teritoriālās ierobežošanas pienākumu, jo tajā nav prasīts, lai datu glabāšana vai apstrāde tiktu veikta Savienībā.

(83) Kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, būtu jāspēj sniegt IKT pakalpojumus no jebkuras vietas pasaulē, ne obligāti vai ne tikai no telpām, kas atrodas Savienībā. Pārraudzības darbības vispirms būtu jāveic telpās, kas atrodas Savienībā, un mijiedarbojoties ar vienībām, kas atrodas Savienībā, tostarp ar meitasuzņēmumiem, kurus, ievērojot šo regulu, izveidojušas kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus. Tomēr šādas darbības Savienībā varētu būt nepietiekamas, lai galvenais pārraugs varētu pilnībā un efektīvi pildīt savus pienākumus saskaņā ar šo regulu. Tāpēc galvenajam pārraugam būtu jāspēj īstenot savas attiecīgās pārraudzības pilnvaras arī trešās valstīs. Minēto pilnvaru īstenošanai trešās valstīs būtu jāsniedz galvenajam pārraugam iespēja pārbaudīt objektus, no kuriem kritiski svarīgā trešā persona, kas sniedz IKT pakalpojumus, faktiski nodrošina vai pārvalda IKT pakalpojumus vai tehniskā atbalsta pakalpojumus, un būtu jāsniedz galvenajam pārraugam visaptveroša un operacionāla izpratne par kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, IKT riska pārvaldību. Galvenā pārrauga – kā Savienības aģentūras – iespējai īstenot pilnvaras ārpus Savienības teritorijas vajadzētu būt pienācīgi regulētai ar attiecīgiem nosacījumiem, jo īpaši ar attiecīgās kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, piekrišanu. Tāpat attiecīgās trešās valsts iestādes būtu jāinformē par galvenā pārrauga darbību veikšanu to teritorijā, un būtu jāsaņem to piekrišana. Tomēr, lai nodrošinātu efektīvu īstenošanu un neskarot Savienības iestāžu un dalībvalstu attiecīgās kompetences, šādas

([21]) Eiropas Parlamenta un Padomes Direktīva 2013/34/ES (2013. gada 26. jūnijs) par noteiktu veidu uzņēmumu gada finanšu pārskatiem, konsolidētajiem finanšu pārskatiem un saistītiem ziņojumiem, ar ko groza Eiropas Parlamenta un Padomes Direktīvu 2006/43/EK un atceļ Padomes Direktīvas 78/660/EEK un 83/349/EEK (OV L 182, 29.6.2013., 19. lpp.).

pilnvaras ir pilnībā jānostiprina arī, noslēdzot administratīvās sadarbības nolīgumus ar attiecīgās trešās valsts attiecīgajām iestādēm. Tādēļ šai regulai būtu jāļauj EUI noslēgt administratīvās sadarbības nolīgumus ar attiecīgajām trešo valstu iestādēm, kam citādi nevajadzētu radīt juridiskas saistības attiecībā uz Savienību un tās dalībvalstīm.

(84) Lai atvieglotu saziņu ar galveno pārraugu un nodrošinātu pienācīgu pārstāvību, kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus un ir daļa no grupas, par savu koordinācijas punktu būtu jāizraugās viena juridiska persona.

(85) Pārraudzības sistēmai nebūtu jāskar dalībvalstu kompetenci veikt savus pārraudzības vai uzraudzības uzdevumus attiecībā uz trešām personām, kas sniedz IKT pakalpojumus un kuras nav izraudzītas par kritiski svarīgām saskaņā ar šo regulu, bet kuras var uzskatīt par svarīgām valsts līmenī.

(86) Lai izmantotu finanšu pakalpojumu jomas 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. Tai būtu jāsaņem atbalsts no jaunas apakškomitejas (Pārraudzības forums), kas veic sagatavošanās darbus gan attiecībā uz atsevišķām kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, adresētiem lēmumiem, gan kolektīvu ieteikumu izsniegšanu, jo īpaši attiecībā uz kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, pārraudzības programmu salīdzinošo novērtēšanu un IKT koncentrācijas riska jautājumu risināšanas labākās prakses noteikšanu.

(87) Lai nodrošinātu, ka kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, tiek pienācīgi un efektīvi pārraudzītas Savienības līmenī, šajā regulā ir paredzēts, ka jebkuru no trim EUI varētu izraudzīties par galveno pārraugu. Kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, individuālai piešķiršanai vienai no trim EUI būtu jāizriet no to finanšu vienību dominējošā stāvokļa novērtējuma, kuras darbojas finanšu nozarēs, par kurām minētā EUI ir atbildīga. Šai pieejai būtu jānodrošina līdzsvarots uzdevumu un pienākumu sadalījums starp trim EUI saistībā ar pārraudzības funkciju veikšanu un pēc iespējas labāk jāizmanto cilvēkresursi un tehniskās zināšanas, kas pieejamas katrā no trim EUI.

(88) Galvenajiem pārraugiem vajadzētu būt piešķirtām vajadzīgajām pilnvarām veikt kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, izmeklēšanu un pārbaudes uz vietas un neklātienē to telpās un atrašanās vietās un iegūt pilnīgu un atjauninātu informāciju. Minētajām pilnvarām būtu jāļauj galvenajam pārraugam gūt patiesu priekšstatu par finanšu vienībām un Savienības finanšu sistēmai radītā, ar trešo personu saistītā IKT riska veidu, apmēru un ietekmi. Galvenās pārraudzības lomas uzticēšana EUI ir priekšnoteikums, lai izprastu un risinātu IKT riska sistēmisko dimensiju finanšu jomā. Kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, ietekme uz Savienības finanšu nozari un iespējamās problēmas, ko rada ar IKT koncentrāciju saistītais risks, prasa īstenot kolektīvu pieeju Savienības līmenī. Vairāku revīziju vienlaicīga veikšana un piekļuves tiesību izmantošana, ko īsteno vairākas kompetentās iestādes atsevišķi ar nelielu koordināciju vai vispār bez tās, neļautu finanšu uzraudzības iestādēm iegūt pilnīgu un visaptverošu pārskatu par trešās personas, kas sniedz IKT pakalpojumus, risku Savienībā, vienlaikus radot arī dublēšanos, slogu un sarežģītību kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, ja uz tām attiektos daudzi uzraudzības un pārbaudes pieprasījumi.

(89) Ņemot vērā būtisko ietekmi, ko rada izraudzīšana par kritiski svarīgu, šai regulai būtu jānodrošina, ka visā pārraudzības sistēmas īstenošanā tiek ievērotas kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, tiesības. Pirms šādi pakalpojumu sniedzēji tiek izraudzīti par kritiski svarīgiem, tiem, piemēram, vajadzētu būt tiesībām iesniegt galvenajam pārraugam pamatotu paziņojumu, kurā ietverta jebkāda ar to izraudzīšanu saistīta būtiska informācija novērtējuma vajadzībām. Tā kā galvenajam pārraugam vajadzētu būt pilnvarotam sniegt ieteikumus par IKT riska jautājumiem un piemērotiem to novēršanas pasākumiem, ietverot pilnvaras iebilst pret konkrētu līgumisku vienošanos, kas ietekmē finanšu vienības vai finanšu sistēmas stabilitāti, kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, arī būtu jādod iespēja pirms minēto ieteikumu pabeigšanas sniegt paskaidrojumus par ieteikumā paredzēto risinājumu paredzamo ietekmi uz klientiem, kas ir vienības, kuras neietilpst šīs regulas

darbības jomā, un formulēt risinājumus risku mazināšanai. Kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus un nepiekrīt ieteikumiem, būtu jāiesniedz pamatots paskaidrojums par savu nodomu neapstiprināt ieteikumu. Ja šāds pamatots paskaidrojums nav iesniegts vai ja to uzskata par nepietiekamu, galvenajam pārraugam būtu jāizdod publisks paziņojums, kurā īsumā aprakstīta neatbilstība.

(90) Kompetentajām iestādēm savās darbībās attiecībā uz finanšu vienību prudenciālo uzraudzību būtu pienācīgi jāiekļauj uzdevums pārbaudīt galvenā pārrauga sniegto ieteikumu faktisku ievērošanu. Kompetentajām iestādēm būtu jāspēj pieprasīt finanšu vienībām veikt papildu pasākumus, lai novērstu riskus, kas identificēti galvenā pārrauga ieteikumos, un tām būtu savlaicīgi jāizdod paziņojumi šajā sakarā. Ja galvenais pārraugs adresē ieteikumus kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus un kuras tiek uzraudzītas saskaņā ar Direktīvu (ES) 2022/2555, kompetentajām iestādēm būtu jāspēj brīvprātīgi un pirms papildu pasākumu pieņemšanas apspriesties ar kompetentajām iestādēm saskaņā ar minēto direktīvu, lai veicinātu koordinētu pieeju attiecībā uz attiecīgajām kritiski svarīgajām trešām personām, kas sniedz IKT pakalpojumus.

(91) Pārraudzības īstenošanā būtu jāievēro trīs darbības principi, kuru mērķis ir nodrošināt: a) ciešu koordināciju EUI starpā to galveno pārraugu lomās, izmantojot kopīgu pārraudzības tīklu (*JON*), b) atbilstību sistēmai, kas izveidota ar Direktīvu (ES) 2022/2555, (izmantojot brīvprātīgu apspriešanos ar struktūrām saskaņā ar minēto direktīvu, lai izvairītos no tādu pasākumu dublēšanās, kuri vērsti uz kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus), un c) rūpības piemērošanu, lai pēc iespējas samazinātu traucējumu risku pakalpojumiem, ko kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, sniedz klientiem, kuri ir vienības, kas neietilpst šīs regulas darbības jomā.

(92) Pārraudzības sistēmai nebūtu jāaizstāj vai nekādā veidā vai daļā jāaizvieto prasība finanšu vienībām pašām pārvaldīt riskus, ko rada tādu trešo personu izmantošana, kas sniedz IKT pakalpojumus, tostarp to pienākumu pastāvīgi uzraudzīt līgumiskas vienošanās, kas noslēgtas ar kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus. Tāpat pārraudzības sistēmai nebūtu jāietekmē finanšu vienību pilna atbildība par visu šajā regulā un attiecīgajos finanšu pakalpojumu tiesību aktos noteikto juridisko saistību ievērošanu un to izpildi.

(93) Lai izvairītos no dublēšanās un pārklāšanās, kompetentajām iestādēm būtu jāatturas individuāli veikt jebkādus pasākumus, kuru mērķis ir uzraudzīt kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, riskus, un šajā ziņā būtu jāuzticas attiecīgā galvenā pārrauga novērtējumam. Jebkurš pasākums jebkurā gadījumā iepriekš būtu jākoordinē un par to jāvienojas ar galveno pārraugu saistībā ar pārraudzības sistēmas uzdevumu veikšanu.

(94) Lai starptautiskā līmenī veicinātu konverģenci attiecībā uz paraugpraksi, ko izmanto, pārskatot un uzraugot trešo personu, kas sniedz IKT pakalpojumus, digitālo riska pārvaldību, būtu jāmudina EUI noslēgt sadarbības nolīgumus ar attiecīgajām uzraudzības un regulatīvajām trešo valstu iestādēm.

(95) Lai izmantotu to darbinieku īpašās kompetences, tehniskās prasmes un speciālās zināšanas, kuri specializējas operatīvajā un IKT riska jomā kompetentajās iestādēs, trijās EUI un – brīvprātīgi – kompetentajās iestādēs saskaņā ar Direktīvu (ES) 2022/2555, galvenajam pārraugam būtu jāizmanto valstu uzraudzības spējas un zināšanas un jāizveido īpašas pārbaudes grupas katrai kritiski svarīgai trešai personai, kas sniedz IKT pakalpojumus, apvienojot daudznozaru grupas, lai atbalstītu pārraudzības darbību sagatavošanu un izpildi, tostarp kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, vispārējas izmeklēšanas un pārbaudes, kā arī pēc tam veicot jebkurus vajadzīgos turpmākos pasākumus.

(96) Lai gan izmaksas, kas izriet no pārraudzības uzdevumiem, tiktu pilnībā finansētas no maksām, ko iekasē no kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, pirms pārraudzības sistēmas darbības sākuma EUI tomēr, visticamāk, radīsies izmaksas par tādu īpašu IKT sistēmu ieviešanu, kas atbalsta gaidāmo pārraudzību, jo pirms tam būtu jāizstrādā un jāievieš īpašas IKT sistēmas. Tāpēc šajā regulā ir paredzēts hibrīds finansēšanas modelis, saskaņā ar kuru pārraudzības sistēma kā tāda tiktu pilnībā finansēta no maksām, savukārt EUI IKT sistēmu izstrādi finansētu no Savienības un valstu kompetento iestāžu iemaksām.

(97) Kompetentajām iestādēm vajadzētu būt visām prasītajām uzraudzības, izmeklēšanas un sankciju pilnvarām, lai nodrošinātu, ka tās var pienācīgi pildīt savus pienākumus saskaņā ar šo regulu. Principā tām būtu jāpublicē paziņojumi par to piemērotajiem administratīvajiem sodiem. Tā kā finanšu vienības un trešās personas, kas sniedz IKT pakalpojumus, var būt iedibināti dažādās dalībvalstīs un tos var uzraudzīt dažādas kompetentās iestādes, šīs regulas piemērošana būtu jāveicina, no vienas puses, ar ciešu sadarbību starp attiecīgajām kompetentajām iestādēm, tostarp ar ECB attiecībā uz īpašiem uzdevumiem, ko tai uztic saskaņā ar Padomes Regulu (ES) Nr. 1024/2013, un, no otras puses, ar konsultācijām EUI starpā, veicot savstarpēju informācijas apmaiņu un sniedzot palīdzību saistībā ar attiecīgajām uzraudzības darbībām.

(98) Lai turpinātu kvantitatīvi un kvalitatīvi raksturot kritērijus attiecībā uz trešo personu, kas sniedz IKT pakalpojumus, izraudzīšanu par kritiski svarīgām un lai saskaņotu pārraudzības maksas, būtu jādeleģē Komisijai pilnvaras pieņemt aktus saskaņā ar LESD 290. pantu, lai papildinātu šo regulu, sīkāk precizējot sistēmisko ietekmi, kāda trešās personas, kas sniedz IKT pakalpojumus, atteicei vai darbības traucējumam varētu būt uz finanšu vienībām, kurām tā sniedz IKT pakalpojumus, tādu globālo sistēmiski nozīmīgu iestāžu (G-SNI) vai citu sistēmiski nozīmīgu iestāžu (C-SNI) skaitu, kuras paļaujas uz attiecīgo trešo personu, kas sniedz IKT pakalpojumus, aktīvu trešo personu, kas sniedz IKT pakalpojumus, skaitu konkrētajā tirgū, uz izmaksām, kādas ir datu un IKT darba slodzes migrēšanai uz citu 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 ([22]). Jo īpaši, lai deleģēto aktu sagatavošanā nodrošinātu vienādu dalību, Eiropas Parlamentam un Padomei visi dokumenti būtu jāsaņem vienlaicīgi ar dalībvalstu ekspertiem, un minēto iestāžu ekspertiem vajadzētu būt sistemātiskai piekļuvei Komisijas ekspertu grupu sanāksmēm, kurās notiek deleģēto aktu sagatavošana.

(99) Regulatīvajiem tehniskajiem standartiem būtu jānodrošina šajā regulā noteikto prasību konsekventa saskaņošana. Tā kā EUI ir struktūras, kam ir ļoti specializētas zināšanas, tās 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 par būtiskiem ar IKT saistītiem incidentiem, testēšana, kā arī saistībā ar galvenajām prasībām ar trešo personu saistīta IKT riska stabilai uzraudzībai. Komisijai un EUI būtu jānodrošina, lai visas finanšu vienības varētu piemērot minētos standartus un prasības tā, lai piemērošana būtu samērīga ar minēto vienību lielumu un vispārējo riska profilu un pakalpojumu, darbību un operāciju veidu, apmēru un sarežģītību. Komisija būtu jāpilnvaro pieņemt šādus regulatīvos tehniskos standartus, pieņemot deleģēšanas aktus saskaņā ar LESD 290. pantu un saskaņā ar 10.–14. pantu Regulās (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010.

(100) Lai atvieglotu ar IKT saistītu būtisku incidentu un būtisku ar maksājumiem saistītu darbības vai drošības incidentu ziņojumu salīdzināmību, kā arī lai nodrošinātu pārredzamību attiecībā uz līgumisku vienošanos par tādu IKT pakalpojumu izmantošanu, ko sniedz trešās personas, kas sniedz IKT pakalpojumus, EUI būtu jāizstrādā īstenošanas tehnisko standartu projekti, ar kuriem izveido standartizētas veidnes, veidlapas un procedūras finanšu vienībām, ar ko ziņot par būtiskiem ar IKT saistītiem incidentiem un būtiskiem ar maksājumiem saistītiem darbības vai drošības incidentiem, kā arī standartizētas veidnes informācijas reģistram. Izstrādājot minētos standartus, EUI būtu jāņem vērā finanšu vienības lielums un vispārējais riska profils, kā arī tās pakalpojumu, darbību un operāciju veids, apmērs un sarežģītība. Komisija būtu jāpilnvaro pieņemt šādus īstenošanas tehniskos standartus, pieņemot īstenošanas aktus saskaņā ar LESD 291. pantu un saskaņā ar 15. pantu Regulās (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010.

([22]) OV L 123, 12.5.2016., 1. lpp.

(101) Tā kā papildu prasības jau ir noteiktas ar deleģētiem un īstenošanas aktiem, kuru pamatā ir Eiropas Parlamenta un Padomes Regulās (EK) Nr. 1060/2009 ([23]), (ES) Nr. 648/2012 ([24]), (ES) Nr. 600/2014 ([25]) un (ES) Nr. 909/2014 ([26]) 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.

(102) Ņemot vērā to, ka šī regula kopā ar Eiropas Parlamenta un Padomes Direktīvu (ES) Nr. 2022/2556 ([27]) paredz konsolidēt IKT riska pārvaldības noteikumus, kas ir iekļauti vairākās Savienības finanšu pakalpojumu jomas *acquis* regulās un direktīvās, tostarp Eiropas Parlamenta un Padomes Regulās (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011 ([28]), lai nodrošinātu pilnīgu konsekvenci, minētās regulas būtu jāgroza, lai precizētu, ka šajā regulā ir paredzēti piemērojamie ar IKT risku saistītie noteikumi.

(103) Tādēļ ar operacionālo risku saistīto attiecīgo pantu darbības joma, uz kuru pamata Regulās (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011 ir piešķirtas pilnvaras pieņemt deleģētos un īstenošanas aktus, būtu jāsašaurina, lai šajā regulā iekļautu visus noteikumus, kas attiecas uz digitālās darbības noturības aspektiem, kuri pašlaik ir minēto regulu daļa.

(104) Iespējamais sistēmiskais kiberrisks, kas saistīts ar tādu IKT infrastruktūru izmantošanu, kuras nodrošina maksājumu sistēmu darbību un maksājumu apstrādes darbību nodrošināšanu, būtu pienācīgi jārisina Savienības līmenī, izmantojot saskaņotus digitālās noturības noteikumus. Šajā nolūkā Komisijai būtu ātri jāizvērtē nepieciešamība pārskatīt šīs regulas darbības jomu, vienlaikus saskaņojot šādu pārskatīšanu ar Direktīvā (ES) 2015/2366 paredzētās visaptverošās pārskatīšanas rezultātiem. Daudzi plaša mēroga uzbrukumi pēdējo desmit gadu laikā liecina, ka maksājumu sistēmas ir kļuvušas pakļautas kiberdraudiem. Maksājumu sistēmas un maksājumu apstrādes darbības ir ieguvušas būtisku nozīmi Savienības finanšu tirgu darbībā, jo tās ir maksājumu pakalpojumu ķēdes pamatā un tām ir spēcīgas saiknes ar vispārējo finanšu sistēmu. Kiberuzbrukumi šādām sistēmām var izraisīt smagus darbības traucējumus, kas tieši ietekmē ekonomiskās pamatfunkcijas, piemēram, maksājumu atvieglošanu, un netieši ietekmē saistītos ekonomiskos procesus. Kamēr Savienības līmenī nav ieviests saskaņots režīms un maksājumu sistēmu operatoru un apstrādes vienību uzraudzība, dalībvalstis, piemērojot noteikumus maksājumu sistēmu operatoriem un apstrādes vienībām, ko uzrauga to jurisdikcijā, nolūkā piemērot līdzīgu tirgus praksi var iedvesmoties no šajā regulā noteiktajām digitālās darbības noturības prasībām.

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

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

([25]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 600/2014 (2014. gada 15. maijs) par finanšu instrumentu tirgiem un ar ko groza Regulu (ES) Nr. 648/2012 (OV L 173, 12.6.2014., 84. lpp.).

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

([27]) Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2556 (2022. gada 14. decembris), ar ko Direktīvas 2009/65/EK, 2009/138/EK, 2011/61/ES, 2013/36/ES, 2014/59/ES, 2014/65/ES, (ES) 2015/2366 un (ES) 2016/2341 groza attiecībā uz finanšu nozares digitālās darbības noturību (skatīt šā *Oficiālā Vēstneša* 153.. lpp.)

([28]) 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.).

(105) Ņemot vērā to, ka šīs regulas mērķi – proti, augsta digitālās darbības noturības līmeņa sasniegšanu regulētām finanšu vienībām – nevar pietiekami labi sasniegt dalībvalstīs, jo ir jāsaskaņo dažādi atšķirīgi noteikumi Savienības un dalībvalstu tiesībās, 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 minētā mērķa sasniegšanai.

(106) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([29]) 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas 2021. gada 10. maijā ([30]) sniedza atzinumu,

IR PIEŅĒMUŠI ŠO REGULU.

I NODAĻA

Vispārīgi noteikumi

1. pants

Priekšmets

1. Lai sasniegtu augstu kopējo digitālās darbības noturības līmeni, šajā regulā ir noteiktas šādas vienotas prasības attiecībā uz tādu tīklu un informācijas sistēmu drošību, kas atbalsta finanšu vienību uzņēmējdarbības procesus:

a) finanšu vienībām piemērojamās prasības attiecībā uz:

   i) informācijas un komunikācijas tehnoloģiju (IKT) riska pārvaldību;

   ii) ziņošanu par būtiskiem ar IKT saistītiem incidentiem un brīvprātīgu paziņošanu kompetentajām iestādēm par būtiskiem kiberdraudiem;

   iii) 2. panta 1. punkta a)–d) apakšpunktā minēto finanšu vienību ziņošanu kompetentajām iestādēm par būtiskiem ar maksājumiem saistītiem darbības vai drošības incidentiem;

   iv) digitālās darbības noturības testēšanu;

   v) ar kiberdraudiem un ievainojamību saistītu informācijas un izlūkdatu apmaiņu;

   vi) pasākumiem ar trešām personām saistīta IKT riska stabilai pārvaldībai;

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

c) noteikumi par pārraudzības sistēmas izveidi un darbību attiecībā uz trešām personām, kas sniedz kritiski svarīgus IKT pakalpojumus, 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 būtiskas vai svarīgas vienības saskaņā ar valsts noteikumiem, ar kuriem transponē Direktīvas (ES) 2022/2555 3. pantu, šo regulu uzskata kā uz konkrētu nozari attiecināmu Savienības tiesību aktu minētās direktīvas 4. panta vajadzībām.

3. Šī regula neskar dalībvalstu atbildību par būtiskām valsts funkcijām saistībā ar sabiedrisko drošību, aizsardzību un valsts drošību saskaņā ar Savienības tiesību aktiem.

([29]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp.).

([30]) OV C 229, 15.6.2021., 16. lpp.

2. pants

Darbības joma

1. Neskarot 3. un 4. punktu, šo regulu piemēro šādām vienībām:

a) kredītiestādēm;

b) maksājumu iestādēm, tostarp maksājumu iestādēm, kam piemēro atbrīvojumu, ievērojot Direktīvu (ES) 2015/2366;

c) konta informācijas pakalpojumu sniedzējiem;

d) elektroniskās naudas iestādēm, tostarp elektroniskās naudas iestādēm, kam piemēro atbrīvojumu, ievērojot Direktīvu 2009/110/EK;

e) ieguldījumu brokeru sabiedrībām;

f) kriptoaktīvu pakalpojumu sniedzējiem, kas saņēmuši atļauju saskaņā ar Eiropas Parlamenta un Padomes regulu par kriptoaktīvu tirgiem un ar ko groza Regulas (ES) Nr. 1093/2010 un (ES) Nr. 1095/2010 un Direktīvas 2013/36/ES un (ES) 2019/1937 ("regula par kriptoaktīvu tirgiem"), un aktīviem piesaistītu žetonu emitentiem;

g) centrālajiem vērtspapīru depozitārijiem;

h) centrālajiem darījumu partneriem;

i) tirdzniecības vietām;

j) darījumu reģistriem;

k) alternatīvo ieguldījumu fondu pārvaldniekiem;

l) pārvaldības sabiedrībām;

m) datu ziņošanas pakalpojumu sniedzējiem;

n) apdrošināšanas un pārapdrošināšanas sabiedrībām;

o) apdrošināšanas starpniekiem, pārapdrošināšanas starpniekiem un apdrošināšanas papildpakalpojuma starpniekiem;

p) arodpensiju kapitāla uzkrāšanas iestādēm;

q) kredītreitingu aģentūrām;

r) kritiski svarīgu etalonu administratoriem;

s) kolektīvās finansēšanas pakalpojumu sniedzējiem;

t) vērtspapīrošanas repozitorijiem;

u) trešām personām, kas sniedz IKT pakalpojumus.

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

3. Šo regulu nepiemēro:

a) alternatīvo ieguldījumu fondu pārvaldniekiem, kā minēts Direktīvas 2011/61/ES 3. panta 2. punktā;

b) apdrošināšanas sabiedrībām un pārapdrošināšanas sabiedrībām, kā minēts Direktīvas 2009/138/EK 4. pantā;

c) arodpensijas kapitāla uzkrāšanas iestādēm, kas pārvalda pensiju plānus, kuros kopā nav vairāk par 15 dalībniekiem;

d) fiziskām vai juridiskām personām, kam piemēro atbrīvojumu, ievērojot Direktīvas 2014/65/ES 2. un 3. pantu;

e) apdrošināšanas starpniekiem, pārapdrošināšanas starpniekiem un apdrošināšanas papildpakalpojuma starpniekiem, kas ir mikrouzņēmumi vai mazie vai vidējie uzņēmumi;

f) pasta žiro norēķinu iestādēm, kā minēts Direktīvas 2013/36/ES 2. panta 5. punkta 3) apakšpunktā.

4. Dalībvalstis var izslēgt no šīs regulas darbības jomas vienības, kas minētas Direktīvas 2013/36/ES 2. panta 5. punkta 4.–23. apakšpunktā un kas atrodas to attiecīgajās teritorijās. Ja dalībvalsts izmanto šādu iespēju, tā informē Komisiju par to, kā arī par jebkādām turpmākām izmaiņām šajā sakarā. Komisija minēto informāciju dara publiski pieejamu savā tīmekļa vietnē vai citā viegli pieejamā veidā.

3. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "digitālās darbības noturība" ir finanšu vienības spēja veidot, nodrošināt un pārskatīt savu darbības integritāti un uzticamību, tieši vai netieši, izmantojot pakalpojumus, ko sniedz trešās personas, kas sniedz IKT pakalpojumus, 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, tostarp traucējumu laikā;

2) "tīklu un informācijas sistēma" ir tīklu un informācijas sistēma, kā definēts Direktīvas (ES) 2022/2555 6. panta 1. punktā;

3) "mantota IKT sistēma" ir IKT sistēma, kas ir sasniegusi sava aprites cikla beigas (ekspluatācijas laika beigas), kas nav piemērota modernizācijai vai labošanai tehnoloģisku vai komerciālu iemeslu dēļ vai ko vairs neatbalsta tās piegādātājs vai trešā persona, kas sniedz IKT pakalpojumus, bet kura joprojām tiek izmantota un atbalsta finanšu vienības funkcijas;

4) "tīklu un informācijas sistēmu drošība" ir tīklu un informācijas sistēmu drošība, kā definēts Direktīvas (ES) 2022/2555 6. panta 2. punktā;

5) "IKT risks" ir jebkāds ar tīklu un informācijas sistēmu izmantošanu saistīts un saprātīgi identificējams apstāklis, kas īstenošanās gadījumā varētu apdraudēt tīklu un informācijas sistēmu, jebkura no tehnoloģijām atkarīga rīka vai procesa, darbības un noritošo procesu vai pakalpojumu sniegšanas drošību, radot negatīvas sekas digitālajā vai fiziskajā vidē;

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

7) "IKT aktīvs" ir programmatūras vai aparatūras aktīvs tīklu un informācijas sistēmās, ko izmanto finanšu vienība;

8) "ar IKT saistīts incidents" ir atsevišķs incidents vai savstarpēji saistītu notikumu virkne, ko finanšu vienība nav plānojusi un kas apdraud drošību tīklu un informācijas sistēmās, un negatīvi ietekmē datu pieejamību, autentiskumu, integritāti vai konfidencialitāti vai finanšu vienības sniegtos pakalpojumus;

9) "ar maksājumiem saistīts darbības vai drošības incidents" ir atsevišķs notikums vai savstarpēji saistītu notikumu virkne, ko neplāno 2. panta 1. punkta a)–d) apakšpunktā minētās finanšu vienības, neatkarīgi no tā, vai tas ir vai nav saistīts ar IKT, un kas negatīvi ietekmē ar maksājumiem saistīto datu pieejamību, autentiskumu, integritāti vai konfidencialitāti vai ar maksājumiem saistītos finanšu vienības sniegtos pakalpojumus;

10) "būtisks ar IKT saistīts incidents" ir ar IKT saistīts incidents, kam ir liela nelabvēlīga ietekme uz tīklu un informācijas sistēmām, kas atbalsta finanšu vienības kritiski svarīgas vai svarīgas funkcijas;

11) "būtisks ar maksājumiem saistīts darbības vai drošības incidents" ir ar maksājumiem saistīts darbības vai drošības incidents, kam ir liela nelabvēlīga ietekme uz sniegtajiem pakalpojumiem, kas saistīti ar maksājumiem;

12) "kiberdraudi" ir kiberdraudi, kā definēts Regulas (ES) 2019/881 2. panta 8. punktā;

13) "būtiski kiberdraudi" ir kiberdraudi, kuru tehniskās īpašības norāda, ka tie varētu izraisīt būtisku ar IKT saistītu incidentu vai būtisku ar maksājumiem saistītu darbības vai drošības incidentu;

14) "kiberuzbrukums" ir ļaunprātīgs ar IKT saistīts incidents, kas ir izraisīts, mēģinot iznīcināt, pakļaut, mainīt, atspējot, nozagt aktīvu vai iegūt neatļautu piekļuvi aktīvam, vai neatļauti izmantot aktīvu, un ko veic jebkurš apdraudējuma dalībnieks;

15) "draudu izlūkdati" ir informācija, kas apkopota, pārveidota, analizēta, interpretēta vai papildināta, lai nodrošinātu vajadzīgo kontekstu lēmumu pieņemšanai un lai ļautu panākt 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;

16) "ievainojamība" ir aktīva, sistēmas, procesa vai kontroles trūkums, uzņēmība vai nepilnība, ko var izmantot;

17) "draudu vadīta ielaušanās testēšana (DVIT)" 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) finanšu vienības kritiski svarīgas aktīvas izstrādes sistēmas testēšanu;

18) "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 tās apakšuzņēmēju sniegtus IKT pakalpojumus, tostarp ar ārpakalpojumu līgumu starpniecību;

19) "trešā persona, kas sniedz IKT pakalpojumus" ir uzņēmums, kas sniedz IKT pakalpojumus;

20) "IKT pakalpojumu sniedzēji, kuri pieder vienai grupai" ir uzņēmums, kas pieder finanšu grupai un galvenokārt sniedz IKT pakalpojumus tās pašas grupas finanšu vienībām vai finanšu vienībām, uz kurām attiecas tā pati institucionālā aizsardzības shēma, tostarp mātesuzņēmumiem, meitasuzņēmumiem, filiālēm vai citām vienībām, kas pakļautas tām pašām īpašumtiesībām vai kontrolei;

21) "IKT pakalpojumi" ir digitālie un datu pakalpojumi, ko ar IKT sistēmu starpniecību pastāvīgi sniedz vienam vai vairākiem iekšējiem vai ārējiem lietotājiem, tostarp aparatūras nodrošināšanas pakalpojumi un ar aparatūru saistīti pakalpojumi, kas ietver tehniskā atbalsta sniegšanu, izmantojot programmatūru vai aparātprogrammatūras atjauninājumus, ko veic aparatūras nodrošinātājs, izņemot tradicionālos analogās telefonijas pakalpojumus;

22) "kritiski svarīga vai svarīga funkcija" ir funkcija, kuras traucējums būtiski pasliktinātu finanšu vienības finanšu darbības rezultātus vai tās pakalpojumu un darbību stabilitāti vai nepārtrauktību, vai 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;

23) "kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus" ir trešā persona, kas sniedz IKT pakalpojumus un kura ir izraudzīta par kritiski svarīgu saskaņā ar 31. pantu;

24) "trešā valstī iedibināta trešā persona, kas sniedz IKT pakalpojumus" ir trešā persona, kas sniedz IKT pakalpojumus un kas ir trešā valstī iedibināta juridiska persona, kura ir noslēgusi līgumisku vienošanos ar finanšu vienību par IKT pakalpojumu sniegšanu;

25) "meitasuzņēmums" ir meitasuzņēmums Direktīvas 2013/34/ES 2. panta 10. punkta un 22. panta nozīmē;

26) "grupa" ir grupa, kā definēts Direktīvas 2013/34/ES 2. panta 11. punktā;

27) "mātesuzņēmums" ir mātesuzņēmums Direktīvas 2013/34/ES 2. panta 9. punkta un 22. panta nozīmē;

28) "trešā valstī iedibināts IKT apakšuzņēmējs" ir IKT apakšuzņēmējs, kas ir trešā valstī iedibināta juridiska persona un kas ir noslēdzis līgumisku vienošanos vai nu ar trešo personu, kas sniedz IKT pakalpojumus, vai ar trešā valstī iedibinātu trešo personu, kas sniedz IKT pakalpojumus;

29) "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 iespējami apdraudēt finanšu vienības spēju nodrošināt kritiski svarīgas vai svarīgas funkcijas vai likt ciest cita veida nelabvēlīgas sekas, tostarp lielus zaudējumus, vai apdraudēt Savienības finansiālo stabilitāti kopumā;

30) "vadības struktūra" ir vadības struktūra, kā definēts Direktīvas 2014/65/ES 4. panta 1. punkta 36) apakšpunktā, Direktīvas 2013/36/ES 3. panta 1. punkta 7) apakšpunktā, Eiropas Parlamenta un Padomes Direktīvas 2009/65/EK ([31]) 2. panta 1. punkta s) apakšpunktā, Regulas (ES) Nr. 909/2014 2. panta 1. punkta 45) apakšpunktā, Regulas (ES) 2016/1011 3. panta 1. punkta 20) apakšpunktā un Regulas par kriptoaktīvu tirgiem attiecīgajā noteikumā, vai līdzvērtīgās personas, kas faktiski vada vienību vai pilda galvenās funkcijas saskaņā ar attiecīgajiem Savienības vai valsts tiesību aktiem;

31) "kredītiestāde" ir kredītiestāde, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) Nr. 575/2013 ([32]) 4. panta 1. punkta 1. apakšpunktā;

32) "iestāde, kam piemēro atbrīvojumu, ievērojot Direktīvu 2013/36/ES" ir vienība, kas minēta Direktīvas 2013/36/ES 2. panta 5. punkta 4)–23) apakšpunktā;

33) "ieguldījumu brokeru sabiedrība" ir ieguldījumu brokeru sabiedrība, kā definēts Direktīvas 2014/65/ES 4. panta 1. punkta 1. apakšpunktā;

34) "neliela un savstarpēji nesaistīta ieguldījumu brokeru sabiedrība" ir ieguldījumu brokeru sabiedrība, kas atbilst nosacījumiem, kuri izklāstīti Eiropas Parlamenta un Padomes Regulas (ES) 2019/2033 ([33]) 12. panta 1. punktā;

35) "maksājumu iestāde" ir maksājumu iestāde, kā definēts Direktīvas (ES) 2015/2366 4. panta 4. punktā;

36) "maksājumu iestāde, kam piemēro atbrīvojumu, ievērojot Direktīvu (ES) 2015/2366" ir maksājumu iestāde, kam piemēro atbrīvojumu, ievērojot Direktīvas (ES) 2015/2366 32. panta 1. punktu;

37) "konta informācijas pakalpojumu sniedzējs" ir konta informācijas pakalpojumu sniedzējs, kā minēts Direktīvas (ES) 2015/2366 33. panta 1. punktā;

38) "elektroniskās naudas iestāde" ir elektroniskās naudas iestāde, kā definēts Eiropas Parlamenta un Padomes Direktīvas 2009/110/EK 2. panta 1. punktā;

39) "elektroniskās naudas iestāde, kam piemēro atbrīvojumu, ievērojot Direktīvu 2009/110/EK" ir elektroniskās naudas iestāde, kam piemēro atbrīvojumu, ievērojot Direktīvas 2009/110/EK 9. panta 1. punktu;

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

41) "darījumu reģistrs" ir darījumu reģistrs, kā definēts Regulas (ES) Nr. 648/2012 2. panta 2. punktā;

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

43) "tirdzniecības vieta" ir tirdzniecības vieta, kā definēts Direktīvas 2014/65/ES 4. panta 1. punkta 24. apakšpunktā;

44) "alternatīvo ieguldījumu fondu pārvaldnieks" ir alternatīvo ieguldījumu fondu pārvaldnieks, kā definēts Direktīvas 2011/61/ES 4. panta 1. punkta b) apakšpunktā;

45) "pārvaldības sabiedrība" ir pārvaldības sabiedrība, kā definēts Direktīvas 2009/65/EK 2. panta 1. punkta b) apakšpunktā;

46) "datu ziņošanas pakalpojumu sniedzējs" ir datu ziņošanas pakalpojumu sniedzējs Regulas (ES) Nr. 600/2014 nozīmē, kā minēts tās 2. panta 1. punkta 34)–36) apakšpunktā;

47) "apdrošināšanas sabiedrība" ir apdrošināšanas sabiedrība, kā definēts Direktīvas 2009/138/EK 13. panta 1. punktā;

48) "pārapdrošināšanas sabiedrība" ir pārapdrošināšanas sabiedrība, kā definēts Direktīvas 2009/138/EK 13. panta 4. punktā;

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

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

([33]) Eiropas Parlamenta un Padomes Regula (ES) 2019/2033 (2019. gada 27. novembris) par prudenciālajām prasībām ieguldījumu brokeru sabiedrībām un ar ko groza Regulas (ES) Nr. 1093/2010, (ES) Nr. 575/2013, (ES) Nr. 600/2014 un (ES) Nr. 806/2014 (OV L 314, 5.12.2019., 1. lpp.).

49) "apdrošināšanas starpnieks" ir apdrošināšanas starpnieks, kā definēts Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/97 ([34]) 2. panta 1. punkta 3) apakšpunktā;

50) "apdrošināšanas papildpakalpojuma starpnieks" ir apdrošināšanas papildpakalpojuma starpnieks, kā definēts Direktīvas (ES) 2016/97 2. panta 1. punkta 4) apakšpunktā;

51) "pārapdrošināšanas starpnieks" ir pārapdrošināšanas starpnieks, kā definēts Direktīvas (ES) 2016/97 2. panta 1. punkta 5) apakšpunktā;

52) "arodpensijas kapitāla uzkrāšanas institūcija" ir arodpensijas kapitāla uzkrāšanas institūcija, kā definēts Direktīvas (ES) 2016/2341 6. panta 1. punktā;

53) "neliela arodpensijas kapitāla uzkrāšanas institūcija" ir arodpensijas kapitāla uzkrāšanas institūcija, kas pārvalda pensiju plānus, kuros kopā ir mazāk nekā 100 dalībnieku;

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

55) "kriptoaktīvu pakalpojumu sniedzējs" ir kriptoaktīvu pakalpojumu sniedzējs, kā definēts Regulas par kriptoaktīvu tirgiem attiecīgajā noteikumā;

56) "aktīviem piesaistītu žetonu emitents" ir "aktīviem piesaistītu žetonu" emitents, kā definēts Regulas par kriptoaktīvu tirgiem attiecīgajā noteikumā;

57) "kritiski svarīgu etalonu administrators" ir "kritiski svarīgu etalonu" administrators, kā definēts Regulas (ES) 2016/1011 3. panta 1. punkta 25) apakšpunktā;

58) "kolektīvās finansēšanas pakalpojumu sniedzējs" ir kolektīvās finansēšanas pakalpojumu sniedzējs, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) 2020/1503 ([35]) 2. panta 1. punkta e) apakšpunktā;

59) "vērtspapīrošanas repozitorijs" ir vērtspapīrošanas repozitorijs, kā definēts Eiropas Parlamenta un Padomes Regulas (ES) 2017/2402 ([36]) 2. panta 23. punktā;

60) "mikrouzņēmums" ir finanšu vienība, kura nav tirdzniecības vieta, centrālais darījumu partneris, darījumu reģistrs vai centrālais vērtspapīru depozitārijs un kura nodarbina mazāk nekā 10 personas un kuras gada apgrozījums un/vai kopējā gada bilance nepārsniedz 2 miljonus EUR;

61) "galvenais pārraugs" ir Eiropas Uzraudzības iestāde, kas izraudzīta saskaņā ar šīs regulas 31. panta 1. punkta b) apakšpunktu;

62) "apvienotā komiteja" ir komiteja, kas minēta Regulu (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010 54. pantā;

63) "mazais uzņēmums" ir finanšu vienība, kura nodarbina 10 vai vairāk personas, bet mazāk nekā 50 personas, un kuras gada apgrozījums un/vai kopējā gada bilance pārsniedz 2 miljonus EUR, bet nepārsniedz 10 miljonus EUR;

64) "vidējais uzņēmums" ir finanšu vienība, kura nav mazais uzņēmums un kura nodarbina mazāk nekā 250 personas un kuras gada apgrozījums nepārsniedz 50 miljonus EUR un/vai gada bilance nepārsniedz 43 miljonus EUR;

65) "publiska iestāde" ir jebkura valdības vai cita valsts pārvaldes struktūra, tostarp valstu centrālās bankas.

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

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

([36]) Eiropas Parlamenta un Padomes Regula (ES) 2017/2402 (2017. gada 12. decembris), ar ko nosaka vispārēju regulējumu vērtspapīrošanai un izveido īpašu satvaru attiecībā uz vienkāršu, pārredzamu un standartizētu vērtspapīrošanu, un groza Direktīvas 2009/65/EK, 2009/138/EK un 2011/61/ES un Regulas (EK) Nr. 1060/2009 un (ES) Nr. 648/2012 (OV L 347, 28.12.2017., 35. lpp.).

4. pants

Proporcionalitātes princips

1. Finanšu vienības II nodaļā paredzētos noteikumus īsteno saskaņā ar proporcionalitātes principu, ņemot vērā savu lielumu un vispārējo rika profilu, kā arī savu pakalpojumu, darbību un operāciju veidu, apmēru un sarežģītību.

2. Turklāt tas, kā finanšu vienības piemēro III un IV nodaļu un V nodaļas I iedaļu, ir proporcionāls to lielumam un vispārējam riska profilam, kā arī to pakalpojumu, darbību un operāciju veidam, apmēram un sarežģītībai, kā konkrēti noteikts minēto nodaļu attiecīgajos noteikumos.

3. Kad kompetentās iestādes pārskata IKT riska pārvaldības sistēmas saskaņotību, pamatojoties uz ziņojumiem, kas iesniegti pēc kompetento iestāžu pieprasījuma, ievērojot 6. panta 5. punktu un 16. panta 2. punktu, tās ņem vērā to, kā finanšu vienības piemēro proporcionalitātes principu.

II NODAĻA

IKT riska pārvaldība

I iedaļa

5. pants

Pārvaldība un organizācija

1. Finanšu vienībām ir izveidota iekšējās pārvaldības un kontroles sistēma, kas nodrošina IKT riska efektīvu un prudenciālu pārvaldību saskaņā ar 6. panta 4. punktu, lai sasniegtu augstu digitālās darbības noturības līmeni.

2. Finanšu vienības vadības struktūra nosaka, apstiprina, pārrauga un atbild par visu ar 6. panta 1. punktā minēto IKT riska pārvaldības sistēmu saistīto pasākumu īstenošanu:

Pirmās daļas īstenošanas vajadzībām vadības struktūra:

a) uzņemas galīgo atbildību par finanšu vienības IKT riska pārvaldību;

b) ievieš politiku, kuras mērķis ir nodrošināt augstu datu pieejamības, autentiskuma, integritātes un konfidencialitātes standartu uzturēšanu;

c) nosaka visu ar IKT saistīto funkciju uzdevumus un atbildību un izveido atbilstošu pārvaldības kārtību, lai nodrošinātu efektīvu un savlaicīgu saziņu, sadarbību un koordināciju starp minētajām funkcijām;

d) uzņemas vispārēju atbildību par digitālās darbības noturības stratēģijas noteikšanu un apstiprināšanu, kā minēts 6. panta 8. punktā, tostarp par atbilstīgas finanšu vienības IKT riska tolerances līmeņa noteikšanu, kā minēts 6. panta 8. punkta b) apakšpunktā;

e) apstiprina, pārrauga un periodiski pārskata attiecīgi 11. panta 1. un 3. punktā minēto finanšu vienības IKT darbības nepārtrauktības politikas un IKT reaģēšanas un seku novēršanas plānu īstenošanu, kurus var pieņemt kā īpašu politiku, kas ir neatņemama daļa no finanšu vienības vispārējās darbības nepārtrauktības politikas un reaģēšanas un seku novēršanas plāna;

f) apstiprina un periodiski pārskata finanšu vienības IKT iekšējās revīzijas plānus, IKT revīzijas un būtiskus to grozījumus;

g) piešķir un periodiski pārskata atbilstīgu budžetu, lai apmierinātu finanšu vienības digitālās darbības noturības vajadzības attiecībā uz visu veidu resursiem, tostarp uz attiecīgajām IKT drošības izpratnes veidošanas programmām un digitālās darbības noturības mācībām, kas minētas 13. panta 6. punktā, un IKT prasmēm visam personālam;

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

i) korporatīvā līmenī izveido ziņošanas kanālus, kas tai ļauj būt pienācīgi informētai par šādiem jautājumiem:

i) vienošanās, kas noslēgtas ar trešām personām, kas sniedz IKT pakalpojumus, par IKT pakalpojumu izmantošanu,

ii) jebkādas attiecīgās plānotās būtiskās izmaiņas attiecībā uz trešām personām, kas sniedz IKT pakalpojumus,

iii) šādu izmaiņu iespējamo ietekmi uz kritiski svarīgajām vai svarīgajām funkcijām, uz kurām attiecas minētās vienošanās, tostarp riska analīzes kopsavilkumu, lai novērtētu minēto izmaiņu ietekmi, un vismaz par būtiskiem ar IKT saistītiem incidentiem un to ietekmi, kā arī reaģēšanas, seku novēršanas un korektīvajiem pasākumiem.

3. Finanšu vienības, kas nav mikrouzņēmumi, izveido funkciju nolūkā uzraudzīt ar trešām personām, kas sniedz IKT pakalpojumus, noslēgtās vienošanās par IKT pakalpojumu izmantošanu, vai iecelt augstākās vadības locekli, kas atbild par to, lai tiktu uzraudzīta pakļautība riskam un attiecīgie dokumenti.

4. Finanšu vienības vadības struktūras locekļi aktīvi atjaunina pietiekamas zināšanas un prasmes, kas ļauj saprast un novērtēt IKT risku un tā ietekmi uz finanšu vienības darbību, tostarp regulāri apmeklējot īpašas mācības atbilstīgi pārvaldītajam IKT riskam.

II iedaļa

6. pants

IKT riska pārvaldības sistēma

1. Finanšu vienībām ir stabila, visaptveroša un labi dokumentēta IKT riska pārvaldības sistēma, kas veido daļu no viņu vispārējās riska pārvaldīšanas sistēmas un ļauj tām ātri, efektīvi un visaptveroši novērst IKT risku un nodrošināt augstu digitālās darbības noturības līmeni.

2. IKT riska pārvaldības sistēma ietver vismaz stratēģijas, politiku, procedūras, IKT protokolus un rīkus, kas ir vajadzīgi, lai rūpīgi un pienācīgi aizsargātu visus informācijas aktīvus un IKT aktīvus, tostarp datoru programmatūru, aparatūru, serverus, kā arī lai aizsargātu visus attiecīgos fiziskos komponentus un infrastruktūras, piemēram, telpas, datu centrus un sensitīvas noteiktās teritorijas, lai nodrošinātu, ka visi informācijas aktīvi un IKT aktīvi ir pienācīgi aizsargāti pret riskiem, tostarp bojājumiem un neatļautu piekļuvi vai izmantošanu.

3. Saskaņā ar savu IKT riska pārvaldības sistēmu finanšu vienības pēc iespējas samazina IKT riska ietekmi, izmantojot piemērotas stratēģijas, politiku, procedūras, IKT protokolus un rīkus. Tās kompetentajām iestādēm pēc pieprasījuma sniedz pilnīgu un atjauninātu informāciju par IKT risku un par savu IKT riska pārvaldības sistēmu.

4. Finanšu vienības, kas nav mikrouzņēmumi, atbildību par IKT riska pārvaldību un pārraudzību uztic kontroles funkcijai un, lai izvairītos no interešu konfliktiem, nodrošina pienācīgu šīs kontroles funkcijas neatkarības līmeni. Finanšu vienības nodrošina IKT riska pārvaldības funkciju, kontroles funkciju un iekšējās revīzijas funkciju pienācīgu nodalījumu un neatkarību atbilstīgi trīs aizsardzības līniju modelim vai iekšējam riska pārvaldības un kontroles modelim.

5. IKT riska pārvaldības sistēmu dokumentē un pārskata vismaz reizi gadā vai periodiski mikrouzņēmumu gadījumā, 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. Ziņojumu par IKT riska pārvaldības sistēmas pārskatīšanu kompetentajai iestādei iesniedz pēc tās pieprasījuma.

6. Finanšu vienību, kas nav mikrouzņēmumi, IKT riska pārvaldības sistēmai revidenti regulāri veic iekšējo revīziju atbilstīgi finanšu vienību revīzijas plānam. Minētajiem revidentiem ir pietiekamas zināšanas, prasmes un zinātība par IKT risku, kā arī pienācīga neatkarība. IKT revīzijas biežums un tajā galvenokārt pievērstā uzmanība ir samērīga ar finanšu vienības IKT riskam.

7. Pamatojoties uz iekšējās revīzijas pārskata secinājumiem, finanšu vienības izveido oficiālu turpmākās pārraudzības procesu, tostarp noteikumus par kritiski svarīgu IKT revīzijas konstatējumu savlaicīgu verifikāciju un izlabošanu.

8. IKT riska pārvaldības sistēma ietver digitālās darbības noturības stratēģiju, kurā izklāstīts, kā sistēma jāīsteno. Šajā nolūkā digitālās darbības noturības stratēģija ietver metodes, kā novērst IKT risku un sasniegt konkrētus IKT mērķus:

a) izskaidrojot, kā IKT riska pārvaldības sistēma atbalsta finanšu vienības uzņēmējdarbības 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, tostarp galvenos snieguma rādītājus un galvenos riska rādītājus;

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

e) izklāstot dažādos mehānismus, kas ieviesti, lai atklātu ar IKT saistītus incidentus, novērstu to ietekmi un nodrošinātu aizsardzību pret to;

f) pamatojot pašreizējās digitālās darbības noturības situāciju, balstoties uz paziņoto būtisko ar IKT saistīto incidentu skaitu un preventīvo pasākumu efektivitāti;

g) īstenojot digitālās darbības noturības testēšanu saskaņā ar šīs regulas IV nodaļu;

h) izklāstot saziņas stratēģiju ar IKT saistītu incidentu gadījumā, par ko jāsniedz informācija saskaņā ar 14. pantu.

9. Finanšu vienības saistībā ar 8. punktā minēto digitālās darbības noturības stratēģiju var noteikt holistisku IKT vairāku piegādātāju stratēģiju grupas vai vienības līmenī, norādot svarīgākās atkarības no trešām personām, kas sniedz IKT pakalpojumus, un izskaidrojot trešo personu, kas sniedz pakalpojumus, iepirkuma loka pamatojumu.

10. Finanšu vienības saskaņā ar Savienības un valsts nozaru tiesību aktiem var IKT riska pārvaldības prasību izpildes pārbaudes uzdevumus kā ārpakalpojumu uzticēt grupas iekšienē vai ārējiem uzņēmumiem. Šādu ārpakalpojumu gadījumā finanšu vienība joprojām ir pilnībā atbildīga par IKT riska pārvaldības prasību izpildes pārbaudi.

7. pants

IKT sistēmas, protokoli un rīki

Lai novērstu un pārvaldītu IKT risku, finanšu vienības izmanto un uztur atjauninātas IKT sistēmas, protokolus un rīkus, kas ir:

a) piemēroti to operāciju apjomam, ar kurām tiek atbalstīta to darbība, saskaņā ar 4. pantā minēto proporcionalitātes principu;

b) uzticami;

c) aprīkoti ar pietiekamu veiktspēju, lai precīzi apstrādātu darbību veikšanai un savlaicīgai pakalpojumu sniegšanai nepieciešamos datus, kā arī pēc vajadzības apstrādātu rīkojumu, ziņojumu vai darījumu maksimālos apjomus, tostarp, ja tiek ieviesta jauna tehnoloģija;

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

8. pants

Identifikācija

1. Regulas 6. panta 1. punktā minētās IKT riska pārvaldības sistēmas ietvaros finanšu vienības identificē, klasificē un pienācīgi dokumentē visas IKT atbalstītās uzņēmējdarbības funkcijas, uzdevumus un pienākumus, minēto funkciju atbalstošos informācijas aktīvus un IKT aktīvus, un to uzdevumus un atkarības saistībā ar IKT risku. Finanšu vienības pēc vajadzības, bet ne retāk kā reizi gadā izvērtē šīs klasifikācijas un jebkuru attiecīgo dokumentu piemērotību.

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

3. Finanšu vienības, kas nav mikrouzņēmumi, veic riska novērtējumu pēc katrām būtiskām tīklu un informācijas sistēmas infrastruktūras, procesu vai procedūru izmaiņām, kas ietekmē to IKT atbalstītās uzņēmējdarbības funkcijas, informācijas aktīvus vai IKT aktīvus.

4. Finanšu vienības identificē visus informācijas aktīvus un IKT aktīvus, tostarp tos, kas atrodas attālās vietnēs, tīkla resursus un aparatūras iekārtas, un kartē tās, kuras uzskata par kritiski svarīgām. Tās kartē informācijas aktīvu un IKT aktīvu konfigurāciju, kā arī dažādu informācijas aktīvu un 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, kuri palīdz nodrošināt kritiski svarīgas vai svarīgas funkcijas.

6. Šā panta 1., 4. un 5. punkta nolūkiem finanšu vienības uztur attiecīgos krājumus un atjaunina tos periodiski un katru reizi, kad notiek jebkādas būtiskas izmaiņas, kā minēts 3. punktā.

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

9. 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 drošību un darbību un pēc iespējas samazina IKT riska ietekmi uz IKT sistēmām, ieviešot attiecīgus IKT drošības rīkus, rīcībpolitiku un procedūras.

2. Finanšu vienības izstrādā, sagādā un īsteno IKT drošības rīcībpolitiku, procedūras, protokolus un rīkus, kuru mērķis ir nodrošināt IKT sistēmu noturību, nepārtrauktību un pieejamību, jo īpaši to sistēmu, kuras atbalsta kritiski svarīgu vai svarīgu funkciju izpildi, un uzturēt augstus datu pieejamības, autentiskuma, integritātes un konfidencialitātes standartus neatkarīgi no tā, vai tie tiek glabāti, lietoti vai pārsūtīti.

3. Lai sasniegtu 2. punktā minētos mērķus, finanšu vienības izmanto IKT risinājumus un procesus, kas ir piemēroti saskaņā ar 4. pantu. Minētie IKT risinājumi un procesi:

a) nodrošina datu pārsūtīšanas līdzekļu drošību;

b) pēc iespējas samazina datu bojājumu vai zudumu, neatļautas piekļuves un tehnisko nepilnību, kas varētu kavēt uzņēmējdarbību, risku;

c) novērš datu pieejamības trūkumu, autentiskuma un integritātes aizskārumu, konfidencialitātes pārkāpumus un datu zudumu;

d) nodrošina datu aizsardzību pret riskiem, kas rodas no datu pārvaldības, tostarp sliktas pārvaldības, ar apstrādi saistītiem riskiem un cilvēka kļūdām.

4. Šā panta 6. panta 1. punktā minētās IKT riska pārvaldības sistēmas ietvaros finanšu vienības:

a) izstrādā un dokumentē informācijas drošības politiku, ar ko paredz noteikumus, lai aizsargātu savu un attiecīgā gadījumā klientu datu, informācijas aktīvu un IKT aktīvu pieejamību, autentiskumu, integritāti un konfidencialitāti;

b) saskaņā ar uz risku balstītu pieeju izveido stabilu tīkla un infrastruktūras pārvaldības struktūru, lietojot attiecīgus paņēmienus, metodes un protokolus, kas var ietvert tādu automatizētu mehānismu ieviešanu, ar kuriem izolēt skartos informācijas aktīvus kiberuzbrukuma gadījumā;

c) īsteno rīcībpolitiku, kas ierobežo fizisku vai loģisku piekļuvi informācijas aktīviem un IKT aktīviem un datiem tikai tādā apjomā, kāds ir nepieciešams leģitīmām un atļautām funkcijām un darbībām, un šim nolūkam izveido rīcībpolitikas, procedūru un kontroles pasākumu kopumu, ar ko nosaka piekļuves tiesības un nodrošina to pareizu pārvaldību;

d) īsteno rīcībpolitiku un protokolus, kas paredz spēcīgus autentificēšanas mehānismus, kuri ir balstīti uz attiecīgiem standartiem un īpašām kontroles sistēmām, un aizsardzības pasākumus šifrēšanas atslēgu veidā, ar kurām dati tiek šifrēti, balstoties uz apstiprinātiem datu klasifikācijas un IKT riska novērtējuma procesiem;

e) īsteno dokumentētu IKT izmaiņu, tostarp programmatūras, aparatūras, aparātprogrammatūras komponentu, sistēmu vai drošības parametru, pārvaldības politiku, procedūras un kontroli, kas ir balstītas uz riska novērtēšanas 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 dokumentētu attiecīgu un visaptverošu labojumu un atjauninājumu politiku.

Pirmās daļas b) apakšpunkta vajadzībām finanšu vienības projektē tīkla savienojuma infrastruktūru tā, lai to varētu nekavējoties pārtraukt vai segmentēt nolūkā pēc iespējas samazināt kaitīgas ietekmes izplatīšanos, jo īpaši attiecībā uz savstarpēji savienotiem finanšu procesiem.

Pirmās daļas e) apakšpunkta vajadzībām IKT izmaiņu pārvaldības procesu apstiprina atbilstīga hierarhiskā vadība, un tam ir ieviesti īpaši protokoli.

10. pants

Atklāšana

1. Finanšu vienības saskaņā ar 17. pantu ievieš mehānismus, lai nekavējoties atklātu anomālas darbības, tostarp IKT tīkla veiktspējas problēmas un ar IKT saistītus incidentus, kā arī identificētu iespējamās būtiskās atsevišķu ķēdes punktu kļūdainas darbības.

Visus pirmajā daļā minētos atklāšanas mehānismus regulāri testē saskaņā ar 25. pantu.

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

3. Finanšu vienības atvēl pietiekamus resursus un spējas, ar ko uzraudzīt lietotāju darbības, IKT anomāliju un ar IKT saistīto incidentu, jo īpaši kiberuzbrukumu, iestāšanos.

4. Datu ziņošanas pakalpojumu sniedzējs papildus minētajam ir ieviesis sistēmas, kas ļauj efektīvi pārbaudīt tirdzniecības ziņojumu pilnīgumu, identificēt izlaidumus un acīmredzamas kļūdas, kā arī pieprasīt minēto ziņojumu atkārtotu nosūtīšanu.

11. pants

Reaģēšana un seku novēršana

1. Regulas 6. panta 1. punktā minētās IKT riska pārvaldības sistēmas ietvaros un pamatojoties uz 8. pantā noteiktajām identifikācijas prasībām, finanšu vienības ievieš visaptverošu IKT darbības nepārtrauktības politiku, ko var pieņemt kā īpašu, atsevišķu politiku un kas veido finanšu vienības vispārējas darbības nepārtrauktības politikas neatņemamu daļu.

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

a) nodrošināt finanšu vienības kritiski svarīgo vai svarīgo funkciju nepārtrauktību;

b) ātri, pienācīgi un efektīvi reaģēt uz visiem ar IKT saistītajiem incidentiem un novērst tos tā, lai ierobežotu kaitējumu un par prioritārām noteiktu darbības atsākšanu un seku novēršanu;

c) nekavējoties aktivizēt īpašus plānus, kas ļauj īstenot ierobežošanas pasākumus, procesus un tehnoloģijas, kuri piemēroti katram ar IKT saistīto incidentu veidam un ļauj novērst turpmāku kaitējumu, kā arī pielāgotas reaģēšanas un seku novēršanas procedūras, kas noteiktas saskaņā ar 12. pantu;

d) provizoriski aplēst ietekmi, kaitējumu un zaudējumus;

e) noteikt saziņas un krīzes pārvarēšanas pasākumus, kas nodrošina atjauninātas informācijas nosūtīšanu visam attiecīgajam iekšējam personālam un ārējām ieinteresētajām personām saskaņā ar 14. pantu un tās paziņošanu kompetentajām iestādēm saskaņā ar 19. pantu.

3. Regulas 6. panta 1. punktā minētās IKT riska pārvaldības sistēmas ietvaros finanšu vienības īsteno saistītu IKT reaģēšanas un seku novēršanas plānus, uz kuriem finanšu vienību, kas nav mikrouzņēmumi, gadījumā attiecas neatkarīgas iekšējas revīzijas pārskatīšanas.

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. Kā daļu no vispārējās darbības nepārtrauktības politikas finanšu vienības veic uzņēmējdarbības ietekmes analīzi (UIA) saistībā ar savu pakļautību nopietnu uzņēmējdarbības traucējumu riskam. UIA ietvaros finanšu vienības novērtē nopietnu uzņēmējdarbības traucējumu iespējamo ietekmi, izmantojot kvantitatīvus un kvalitatīvus kritērijus, attiecīgā gadījumā izmantojot iekšējo un ārējo datus un scenāriju analīzi. UIA ņem vērā identificēto un kartēto uzņēmējdarbības funkciju, atbalsta procesu, trešo personu atkarības un informācijas aktīvu svarīgumu un to savstarpējo atkarību. Finanšu vienības nodrošina, ka IKT aktīvi un IKT pakalpojumi tiek izstrādāti un izmantoti pilnīgā saskaņā ar UIA, jo īpaši attiecībā uz to, lai pienācīgi nodrošinātu visu kritiski svarīgo komponentu dublēšanos.

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

a) vismaz reizi gadā, kā arī pēc būtiskām tādu IKT sistēmu izmaiņām, ar kurām atbalsta kritiski svarīgas vai svarīgas funkcijas, testē IKT darbības nepārtrauktības plānus un IKT reaģēšanas un seku novēršanas plānus saistībā ar IKT sistēmām, kas atbalsta visas funkcijas;

b) testē saskaņā ar 14. pantu izveidotos krīzes saziņas plānus.

Pirmās daļas 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 12. pantā noteikto pienākumu izpildei.

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

7. Finanšu vienībām, kas nav mikrouzņēmumi, ir krīzes pārvarēšanas funkcija, kurā IKT darbības nepārtrauktības plānu vai IKT reaģēšanas un seku novēršanas plānu aktivizēšanas gadījumā cita starpā paredz skaidras procedūras, kā pārvaldīt iekšējo un ārējo krīzes saziņu saskaņā ar 14. pantu.

8. Finanšu vienības uztur viegli pieejamu reģistru, kurā ietver pirms traucējuma un traucējuma laikā veiktās darbības, ja ticis aktivizēts IKT darbības nepārtrauktības plāns vai IKT reaģēšanas un seku novēršanas plāns.

9. Centrālais vērtspapīru depozitārijs iesniedz kompetentajām iestādēm IKT darbības nepārtrauktības testu vai līdzīgu izmēģinājumu rezultātu kopijas.

10. Finanšu vienības, kas nav mikrouzņēmumi, pēc kompetento iestāžu pieprasījuma ziņo tām par aplēsēm par kopējām gada izmaksām un zaudējumiem, ko radījuši būtiski ar IKT saistīti incidenti.

11. Saskaņā ar Regulu (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010 16. pantu EUI ar Apvienotās komitejas starpniecību līdz 2024. gada 17. jūlijam izstrādā kopīgas pamatnostādnes attiecībā uz 10. punktā minēto kopējo gada izmaksu un zaudējumu aplēsi.

12. pants

Rezerves kopiju veidošanas politika un procedūras, atjaunošanas un atgūšanas procedūras un metodes

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

a) rezerves kopiju veidošanas politiku un procedūras, kur nosaka to datu tvērumu, kuriem jāveido rezerves kopijas, un rezerves kopiju veidošanas minimālo biežumu, balstoties uz informācijas svarīgumu vai datu konfidencialitātes līmeni;

b) atjaunošanas un atgūšanas procedūras un metodes.

2. Finanšu vienības izveido rezerves sistēmas, ko var aktivizēt saskaņā ar rezerves kopiju veidošanas politiku un procedūrām, kā arī atjaunošanas un atgūšanas procedūrām un metodēm. Rezerves sistēmu aktivizēšana neapdraud tīklu un informācijas sistēmu drošību vai datu pieejamību, autentiskumu, integritāti vai konfidencialitāti. Regulāri veic rezerves kopiju veidošanas procedūru un atjaunošanas, kā arī atgūšanas procedūru un metožu testēšanu.

3. Atjaunojot rezerves kopijas datus, finanšu iestādes izmanto IKT sistēmas, kas ir fiziski un loģiski nošķirtas no avota IKT sistēmas. IKT sistēmas ir droši aizsargātas pret jebkādu neatļautu piekļuvi vai IKT bojājumiem un ļauj laikus atjaunot pakalpojumus, vajadzības gadījumā izmantojot datus un sistēmu rezerves kopijas.

Centrālo darījumu partneru seku novēršanas plāni atļauj atjaunot visus darījumus pārtraukšanas brīdī, lai centrālais darījumu partneris varētu turpināt droši darboties un pabeigt norēķinus paredzētajā dienā.

Datu ziņošanas pakalpojumu sniedzēji papildus uztur pienācīgus resursus un nodrošina rezerves kopijas un atjaunošanas iekārtas, lai jebkurā laikā piedāvātu un uzturētu savus pakalpojumus.

4. Finanšu vienības, kas nav mikrouzņēmumi, uztur rezerves IKT jaudu, kam ir uzņēmējdarbības vajadzību nodrošināšanai pienācīgi resursi, spējas un funkcijas. Mikrouzņēmumi, pamatojoties uz to riska profilu, novērtē vajadzību uzturēt šādu rezerves IKT jaudu.

5. Centrālie vērtspapīru depozitāriji uztur vismaz vienu rezerves apstrādes vietu, kam ir uzņēmējdarbības vajadzību nodrošināšanai pienācīgi resursi, spējas, funkcijas 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 vai svarīgu funkciju 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 vai svarīgu funkciju nepārtrauktību gadījumā, ja galvenā apstrādes vieta ir kļuvusi nepieejama.

6. Nosakot mērķus attiecībā uz katras funkcijas atgūšanas laiku un atgūšanas punktu, finanšu vienības ņem vērā to, vai attiecīgā funkcija ir kritiski svarīga vai svarīga, un 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 vajadzīgās pārbaudes, tostarp vairākas pārbaudes un saskaņošanu, lai nodrošinātu, ka datu integritāte tiek saglabāta visaugstākajā līmenī. Šīs pārbaudes veic arī, atjaunojot datus no ārējām ieinteresētajām personām, lai nodrošinātu, ka sistēmu dati ir savstarpēji sakritīgi.

13. pants

Mācīšanās un attīstība

1. Finanšu vienībām ir spējas un personāls, kas var apkopot informāciju par ievainojamību un kiberdraudiem, ar IKT saistītiem incidentiem, jo īpaši kiberuzbrukumiem, un analizēt ietekmi, kas tiem varētu būt uz to digitālās darbības noturību.

2. Finanšu vienības ievieš ar IKT saistītu incidentu pārskatīšanu gadījumiem, kad būtisks ar IKT saistīts incidents traucē to pamatdarbības; tajā tiek analizēti traucējumu cēloņi un noteikti nepieciešamie uzlabojumi IKT darbībās vai IKT darbības nepārtrauktības politikā, kas minēta 11. pantā.

Finanšu vienības, kas nav mikrouzņēmumi, pēc pieprasījuma paziņo kompetentajām iestādēm par izmaiņām, kas veiktas pēc pirmajā daļā minētās ar IKT saistīto incidentu pārskatīšanas.

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, ja to uzskata par lietderīgu;

c) incidentu eskalācijas efektivitāti finanšu vienībā;

d) iekšējās un ārējās saziņas efektivitāti.

3. IKT riska novērtējuma procesā pastāvīgi iekļauj pieredzi, kas gūta saskaņā ar 26. un 27. 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 IKT darbības nepārtrauktības plānus un IKT reaģēšanas un seku novēršanas plānus, kopā ar attiecīgo informāciju, kas koplietota ar darījumu partneriem un novērtēta uzraudzības pārbaudēs. Minētie konstatējumi ir pamats 6. panta 1. punktā minētās IKT riska pārvaldības sistēmas attiecīgo komponentu pienācīgai pārskatīšanai.

4. Finanšu vienības uzrauga 6. panta 8. punktā noteiktās digitālās darbības noturības stratēģijas īstenošanas efektivitāti. Tās kartē IKT riska 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, jo īpaši saistībā ar kritiski svarīgām vai svarīgām funkcijām, 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. Minētās programmas un mācības attiecas uz visiem darbiniekiem un augstākās vadības darbiniekiem, un to sarežģītības pakāpe ir samērīga ar viņu funkciju jomu. Attiecīgā gadījumā finanšu vienības iekļauj arī trešās personas, kas sniedz IKT pakalpojumus, savās attiecīgajās mācību shēmās saskaņā ar 30. panta 2. punkta i) apakšpunktu.

7. Finanšu vienības, kas nav mikrouzņēmumi, pastāvīgi uzrauga attiecīgo tehnoloģisko attīstību, tostarp lai izprastu šādu jaunu tehnoloģiju ieviešanas iespējamo ietekmi uz IKT drošības prasībām un digitālās darbības noturību. Tās seko jaunākajiem IKT riska pārvaldības procesiem, lai efektīvi apkarotu pašreizējās vai jaunās kiberuzbrukumu formas.

14. pants

Saziņa

1. Regulas 6. panta 1. punktā minētās IKT riska pārvaldības sistēmas ietvaros finanšu vienībām ir krīzes saziņas plāni, kas ļauj vismaz būtiskus ar IKT saistītos incidentus vai ievainojamības atbildīgi atklāt klientiem un darījumu partneriem, kā arī sabiedrībai.

2. IKT riska pārvaldības sistēmas ietvaros finanšu vienības īsteno saziņas politiku attiecībā uz iekšējo personālu un ārējām ieinteresētajām personām. Ar personālu saistītajā saziņas politikā ņem vērā vajadzību nošķirt personālu, kas ir jāinformē, no IKT riska pārvaldībā, jo īpaši par reaģēšanu un seku novēršanu, atbildīgā personāla.

3. Vismaz vienai personai finanšu vienībā ir uzdots īstenot saziņas stratēģiju ar IKT saistītu incidentu gadījumā un šim nolūkam pildīt publisko un mediju funkciju.

15. pants

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

EUI ar Apvienotās komitejas starpniecību, apspriežoties ar Eiropas Savienības Kiberdrošības aģentūru (*ENISA*), izstrādā kopīgu regulatīvo tehnisko standartu projektu, lai:

a) noteiktu papildu elementus, kas jāiekļauj 9. 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 pieejamību, autentiskumu, integritāti un konfidencialitāti, tostarp kriptogrāfijas metodes, un garantētu datu precīzu un ātru pārraidi bez būtiskiem traucējumiem un nepamatotiem kavējumiem;

b) izstrādātu papildu komponentus 9. 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;

c) sīkāk izstrādātu 10. panta 1. punktā noteiktos mehānismus, kas ļautu operatīvi atklāt anomālas darbības, un 10. panta 2. punktā izklāstītos kritērijus, kas ierosina ar IKT saistītu incidentu atklāšanas un reaģēšanas procesus;

d) sīkāk precizētu 11. panta 1. punktā minētās IKT darbības nepārtrauktības politikas komponentus;

e) sīkāk precizētu 11. panta 6. punktā minēto IKT darbības nepārtrauktības plānu testēšanu, lai nodrošinātu, ka šādā testēšanā 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;

f) sīkāk precizētu 11. panta 3. punktā minēto IKT reaģēšanas un seku novēršanas plānu komponentus;

g) sīkāk precizētu 6. panta 5. punktā minētā ziņojuma par IKT riska pārvaldības sistēmas pārskatīšanu saturu un formātu.

Izstrādājot minēto regulatīvo tehnisko standartu projektu, EUI ņem vērā finanšu vienības lielumu un vispārējo riska profilu, kā arī tās pakalpojumu, darbību un operāciju veidu, apmēru un sarežģītību, vienlaikus pienācīgi ņemot vērā visas īpašās iezīmes, kas izriet no darbību atšķirīgā rakstura dažādās finanšu pakalpojumu nozarēs.

EUI iesniedz Komisijai minēto regulatīvo tehnisko standartu projektu līdz 2024. gada 17. janvārim.

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

16. pats

Vienkāršota IKT riska pārvaldības sistēma

1. Šīs regulas 5.–15. pantu nepiemēro nelielām un savstarpēji nesaistītām ieguldījumu brokeru sabiedrībām, maksājumu iestādēm, kam piemēro atbrīvojumu, ievērojot Direktīvu (ES) 2015/2366; iestādēm, kam piemēro atbrīvojumu, ievērojot Direktīvu 2013/36/ES, un attiecībā uz kurām dalībvalstis ir nolēmušas nepiemērot šīs regulas 2. panta 4. punktā minēto iespēju; elektroniskās naudas iestādēm, kam piemēro atbrīvojumu, ievērojot Direktīvu 2009/110/EK; un nelielām arodpensijas kapitāla uzkrāšanas institūcijām.

Neskarot pirmo daļu, tajā uzskaitītās vienības:

a) ievieš un uztur stabilu un dokumentētu IKT riska pārvaldības sistēmu, ar ko sīki izklāsta mehānismus un pasākumus, kuru mērķis ir ātra, efektīva un visaptveroša IKT riska pārvaldība, tostarp attiecīgo fizisko komponentu un infrastruktūru aizsardzība;

b) pastāvīgi uzrauga visu IKT sistēmu drošību un darbību;

c) pēc iespējas samazina IKT riska ietekmi, izmantojot stabilas, noturīgas un atjauninātas IKT sistēmas, protokolus un rīkus, kuri ir piemēroti to darbību nodrošināšanai un pakalpojumu sniegšanai un tīklu un informācijas sistēmās esošo datu pieejamības, autentiskuma, integritātes un konfidencialitātes pienācīgai aizsardzībai;

d) ļauj ātri identificēt un atklāt IKT riska un anomāliju cēloņus tīklu un informācijas sistēmās un ātri rīkoties IKT incidentu gadījumos;

e) nosaka galvenās atkarības no trešām personām, kas sniedz IKT pakalpojumus;

f) nodrošina kritiski svarīgo vai svarīgo funkciju nepārtrauktību, izmantojot darbības nepārtrauktības plānus un reaģēšanas un seku novēršanas pasākumus, kas ietver vismaz rezerves kopiju veidošanas un atjaunošanas pasākumus;

g) regulāri testē f) apakšpunktā minētos plānus un pasākumus, kā arī saskaņā ar a) un c) apakšpunktu īstenoto kontroļu efektivitāti;

h) attiecīgā gadījumā IKT riska novērtēšanas procesā īsteno attiecīgus darbības secinājumus, kas izriet no g) apakšpunktā minētajiem testiem un pēcincidentu analīzes, un saskaņā ar vajadzībām un IKT riska profilu izstrādā IKT drošības izpratnes veidošanas programmas un digitālās darbības noturības mācības personālam un vadībai.

2. IKT riska pārvaldības sistēmu, kas minēta 1. punkta otrās daļas a) apakšpunktā, dokumentē un pārskata periodiski un pēc būtiskiem ar IKT saistītiem incidentiem, ievērojot uzraudzības norādījumus. To pastāvīgi uzlabo, balstoties uz īstenošanas un uzraudzības gaitā gūtajām atziņām. Ziņojumu par IKT riska pārvaldības sistēmas pārskatīšanu kompetentajai iestādei iesniedz pēc tās pieprasījuma.

3. EUI ar Apvienotās komitejas starpniecību, apspriežoties ar *ENISA*, izstrādā kopīgu regulatīvo tehnisko standartu projektu, lai:

a) sīkāk precizētu elementus, kas jāiekļauj 1. punkta otrās daļas a) apakšpunktā minētajā IKT riska pārvaldības sistēmā;

b) sīkāk precizētu elementus, kas saistīti ar 1. punkta otrās daļas c) apakšpunktā minētajām sistēmām, protokoliem un rīkiem IKT riska ietekmes iespējamai samazināšanai, nolūkā nodrošināt tīklu drošību, nodrošināt pienācīgus aizsardzības pasākumus pret ielaušanos un datu ļaunprātīgu izmantošanu un saglabātu datu pieejamību, autentiskumu, integritāti un konfidencialitāti;

c) sīkāk precizētu 1. punkta otrās daļas f) apakšpunktā minēto IKT darbības nepārtrauktības plānu komponentus;

d) sīkāk precizētu noteikumus par darbības nepārtrauktības plānu testēšanu un nodrošinātu 1. punkta otrās daļas g) apakšpunktā minētās kontroles efektivitāti un nodrošinātu, ka šādā testēšanā pienācīgi ņem vērā scenārijus, kuros kritiski svarīgas vai svarīgas funkcijas nodrošināšanas kvalitāte pasliktinās līdz nepieņemamam līmenim vai kad tā nedarbojas;

e) sīkāk precizētu 2. punktā minētā ziņojuma par IKT riska pārvaldības sistēmas pārskatīšanu saturu un formātu.

Izstrādājot minēto regulatīvo tehnisko standartu projektu, EUI ņem vērā finanšu vienības lielumu un vispārējo riska profilu, kā arī tās pakalpojumu, darbību un operāciju veidu, apmēru un sarežģītību.

EUI iesniedz Komisijai minēto īstenošanas tehnisko standartu projektus līdz 2024. gada 17. janvārim.

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

III NODAĻA

Ar IKT saistītu incidentu pārvaldības process, klasifikācija un ziņošana

17. pants

Ar IKT saistītu incidentu pārvaldības process

1. Finanšu vienības nosaka, izveido un īsteno ar IKT saistītu incidentu pārvaldības procesu, lai atklātu ar IKT saistītus incidentus, pārvaldītu tos un ziņotu par tiem.

2. Finanšu vienības reģistrē visus ar IKT saistītos incidentus un būtiskus kiberdraudus. Finanšu vienības izveido attiecīgas procedūras un procesus, lai nodrošinātu ar IKT saistītu incidentu konsekventu un integrētu uzraudzību, apstrādi un turpmāko kontroli, lai nodrošinātu, ka ir identificēti, dokumentēti un novērsti to pamatā esošie cēloņi, lai nepieļautu šādu incidentu atkārtošanos.

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

a) ievieš agrīnās brīdināšanas rādītājus;

b) izveido procedūras ar IKT saistītu incidentu identificēšanai, izsekošanai, reģistrēšanai, kategorizācijai un klasificēšanai atbilstīgi to prioritātei, kā arī skarto pakalpojumu nopietnībai un kritiskumam saskaņā ar 18. panta 1. punktā izklāstītajiem kritērijiem;

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

d) saskaņā ar 14. 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;

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

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

18. pants

Ar IKT saistītu incidentu un kiberdraudu klasifikācija

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

a) to klientu vai finanšu darījumu partneru skaits un/vai relevance, kurus ir skāris ar IKT saistītais incidents un – attiecīgā gadījumā – skarto darījumu apjoms vai skaits, kā arī tas, vai ar IKT saistītais incidents ir ietekmējis reputāciju;

b) ar IKT saistītā incidenta ilgums, tostarp konkrētā pakalpojuma nepieejamība;

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

d) datu zudumi, ko rada ar IKT saistītais incidents, saistībā ar datu pieejamību, autentiskumu, integritāti vai konfidencialitāti;

e) ietekmēto pakalpojumu, tostarp finanšu vienības darījumu un operāciju, kritiskums;

f) ar IKT saistītā incidenta ekonomiskā ietekme, jo īpaši tiešās un netiešās izmaksas un zaudējumi, gan absolūtā, gan relatīvā izteiksmē.

2. Finanšu vienības kiberdraudus klasificē kā nozīmīgus, pamatojoties uz riskam pakļauto pakalpojumu kritiskumu, tostarp finanšu vienības darījumiem un darbībām, par mērķi izvirzīto klientu vai finanšu darījumu partneru skaitu un/vai relevanci un riskam pakļauto teritoriju ģeogrāfisko izplatību.

3. EUI ar Apvienotās komitejas starpniecību un apspriežoties ar ECB un *ENISA* izstrādā kopēju regulatīvo tehnisko standartu projektu, tajā sīkāk nosakot:

a) 1. punktā izklāstītos kritērijus, tostarp būtiskuma robežvērtības, pēc kā noteikt būtiskus ar IKT saistītus incidentus vai – attiecīgā gadījumā – būtiskus ar maksājumiem saistītus darbības vai drošības incidentus, kam piemēro 19. panta 1. punktā paredzēto ziņošanas pienākumu;

b) kritērijus, ko piemēro kompetentās iestādes, lai izvērtētu būtisku ar IKT saistītu incidentu vai – attiecīgā gadījumā – būtisku ar maksājumiem saistītu darbības vai drošības incidentu relevanci attiecīgajām kompetentajām iestādēm citās dalībvalstīs, kā arī sīkāku informāciju no ziņojumiem par būtiskiem ar IKT saistītiem incidentiem vai – attiecīgā gadījumā – būtiskiem ar maksājumiem saistītiem darbības vai drošības incidentiem, kas tiek koplietota ar citām kompetentajām iestādēm, ievērojot 19. panta 6. un 7. punktu;

c) kritērijus, kas izklāstīti šā panta 2. punktā, tostarp augstas būtiskuma robežvērtības būtisku kiberdraudu noteikšanai.

4. Izstrādājot šā panta 3. punktā minēto kopējo regulatīvo tehnisko standartu projektus, EUI ņem vērā 4. panta 2. punktā izklāstītos kritērijus, kā arī starptautiskos standartus, norādījumus un *ENISA* izstrādātās un publicētās specifikācijas, tostarp – attiecīgā gadījumā – citu ekonomikas nozaru specifikācijas. Lai piemērotu 4. panta 2. punktā izklāstītos kritērijus, EUI pienācīgi apsver vajadzību mikrouzņēmumiem un maziem un vidējiem uzņēmumiem mobilizēt pietiekamus resursus un spējas, lai nodrošinātu ar IKT saistītu incidentu ātru pārvaldību.

Minētos kopējo regulatīvo tehnisko standartu projektus EUI iesniedz Komisijai līdz 2024. gada 17. janvārim.

Komisijai tiek deleģētas pilnvaras papildināt šo regulu, pieņemot 3. punktā minētos regulatīvos tehniskos standartus saskaņā ar 10.–14. pantu Regulās (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010.

19. pants

Ziņošana par būtiskiem ar IKT saistītiem incidentiem un brīvprātīga paziņošana par būtiskiem kiberdraudiem

1. Finanšu vienības par būtiskiem ar IKT saistītiem incidentiem ziņo 46. pantā minētajai attiecīgajai kompetentajai iestādei saskaņā ar šā panta 4. punktu.

Ja finanšu vienību uzrauga vairāk nekā viena 46. pantā minētā valsts kompetentā iestāde, dalībvalstis izraugās vienu kompetento iestādi par attiecīgo kompetento iestādi, kas ir atbildīga par šajā pantā paredzēto funkciju un pienākumu izpildi.

Kredītiestādes, kas saskaņā ar Regulas (ES) Nr. 1024/2013 6. panta 4. punktu klasificētas kā nozīmīgas, ziņo par būtiskiem ar IKT saistītiem incidentiem attiecīgajai valsts kompetentajai iestādei, kura izraudzīta saskaņā ar Direktīvas 2013/36/ES 4. pantu un kura nekavējoties nosūta minēto ziņojumu ECB.

Piemērojot šā punkta pirmo daļu, finanšu vienības pēc visas attiecīgās informācijas ievākšanas un analīzes, sagatavo sākotnējo paziņojumu un šā panta 4. punktā minētos ziņojumus, izmantojot 20. pantā minētās veidnes, un iesniedz tos kompetentajai iestādei. Ja tehniska neiespējamība liedz iesniegt sākotnējo paziņojumu, izmantojot veidni, finanšu vienības par to paziņo kompetentajai iestādei, izmantojot alternatīvus līdzekļus.

Sākotnējā paziņojumā un 4. punktā minētajos ziņojumos ietver visu informāciju, kas nepieciešama kompetentajai iestādei, lai noteiktu būtiskā ar IKT saistītā incidenta nozīmīgumu un izvērtētu iespējamo pārrobežu ietekmi.

Neskarot ziņošanu attiecīgajai kompetentajai iestādei, kuru finanšu vienība īsteno, ievērojot pirmo daļu, dalībvalstis var papildus noteikt, ka dažas vai visas finanšu vienības, izmantojot 20. pantā minētās veidnes, sniedz arī sākotnējo paziņojumu un katru no šā panta 4. punktā minētajiem ziņojumiem kompetentajām iestādēm vai datordrošības incidentu reaģēšanas vienībām (*CSIRT*), kas izraudzītas vai izveidotas saskaņā ar Direktīvu (ES) 2022/2555.

2. Finanšu vienības var brīvprātīgi paziņot attiecīgajai kompetentajai iestādei par būtiskiem kiberdraudiem, ja tās uzskata, ka apdraudējums ir būtisks finanšu sistēmai, pakalpojumu lietotājiem vai klientiem. Attiecīgā kompetentā iestāde var sniegt šādu informāciju citām attiecīgajām iestādēm, kas minētas 6. punktā.

Kredītiestādes, kas saskaņā ar Regulas (ES) Nr. 1024/2013 6. panta 4. punktu klasificētas kā nozīmīgas, var brīvprātīgi ziņot par būtiskiem kiberdraudiem attiecīgajai valsts kompetentajai iestādei, kura izraudzīta saskaņā ar Direktīvas 2013/36/ES 4. pantu un kura nekavējoties nosūta minēto ziņojumu ECB.

Dalībvalstis var noteikt, ka minētās finanšu vienības, kuras veic brīvprātīgo paziņošanu saskaņā ar pirmo daļu, var nosūtīt minēto paziņojumu arī *CSIRT*, kas izraudzītas vai izveidotas saskaņā ar Direktīvu (ES) 2022/2555.

3. Ja notiek būtisks ar IKT saistīts incidents, un tas ietekmē klientu finanšu intereses, finanšu vienības, tiklīdz tās par to uzzina, bez nepamatotas kavēšanās informē savus klientus par būtisko ar IKT saistīto incidentu un par pasākumiem, kas veikti, lai mazinātu šā incidenta nelabvēlīgo ietekmi.

Būtiska kiberdrauda gadījumā finanšu vienības attiecīgā gadījumā informē savus klientus, kurus minētais drauds varētu potenciāli ietekmēt, par jebkādiem piemērotiem aizsardzības pasākumiem, ko viņi varētu apsvērt veikt.

4. Finanšu vienības termiņā, kas jānosaka saskaņā ar 20. panta pirmās daļas a) apakšpunkta ii) punktu, attiecīgajai kompetentajai iestādei iesniedz:

a) sākotnējo paziņojumu;

b) starpposma ziņojumu pēc a) apakšpunktā minētā sākotnējā ziņojuma, tiklīdz ir būtiski mainījies sākotnējā incidenta statuss vai ja, pamatojoties uz pieejamo jauno informāciju, ir mainījusies būtiskā ar IKT saistītā incidenta apstrāde, kam attiecīgā 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 ieviesti, un kad ir pieejami faktiskie ietekmes rādītāji, ar ko aizstāt aplēses.

5. Finanšu vienības saskaņā ar Savienības un valsts nozaru tiesību aktiem šajā pantā noteikto ziņošanas pienākumu var nodot trešās puses ārpakalpojumu sniedzējam. Šādas ārpakalpojumu izmantošanas gadījumā finanšu vienība joprojām pilnībā atbild par incidentu paziņošanas prasību izpildi.

6. Saņemot sākotnējo paziņojumu un katru 4. punktā minēto ziņojumu, kompetentā iestāde savlaicīgi sniedz informāciju par būtisko ar IKT saistīto incidentu šādiem saņēmējiem, attiecīgā gadījumā pamatojoties uz to attiecīgajām kompetencēm:

a) EBI, EVTI vai EAAPI;

b) šīs regulas 2. panta 1. punkta a), b) un d) apakšpunktā minēto finanšu vienību gadījumā – ECB;

c) kompetentajām iestādēm, vienotajiem kontaktpunktiem vai *CSIRT*, kas izraudzītas vai izveidotas, attiecīgi, saskaņā ar Direktīvu (ES) 2022/2555.

d) noregulējuma iestādēm, kā minēts Direktīvas 2014/59/ES 3. pantā, un Vienotajai noregulējuma valdei (VNV) attiecībā uz vienībām, kas minētas Eiropas Parlamenta un Padomes Regulas (ES) Nr. 806/2014 ([37]) 7. panta 2. punktā, un attiecībā uz vienībām un grupām, kas minētas Regulas (ES) Nr. 806/2014 7. panta 4. punkta b) apakšpunktā un 5. punktā, ja šāda informācija attiecas uz incidentiem, kas rada risku kritiski svarīgu funkciju nodrošināšanai Direktīvas 2014/59/ES 2. panta 1. punkta 35) apakšpunkta nozīmē; un

e) citām attiecīgām valsts iestādēm saskaņā ar valsts tiesību aktiem.

7. Pēc informācijas saņemšanas saskaņā ar 6. punktu EBI, EVTI vai EAAPI un ECB, apspriežoties ar *ENISA* un sadarbojoties ar attiecīgo kompetento iestādi, novērtē, vai būtiskais ar IKT saistītais incidents ir relevants kompetentajām iestādēm citās dalībvalstīs. Pēc minētā novērtējuma EBI, EVTI vai EAAPI pēc iespējas drīz attiecīgi informē attiecīgās kompetentās iestādes citās dalībvalstīs. 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.

([37]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 806/2014 (2014. gada 15. jūlijs), ar ko izveido vienādus noteikumus un vienotu procedūru kredītiestāžu un noteiktu ieguldījumu brokeru sabiedrību noregulējumam, izmantojot vienotu noregulējuma mehānismu un vienotu noregulējuma fondu, un groza Regulu (ES) Nr. 1093/2010 (OV L 225, 30.7.2014., 1. lpp.).

8. Paziņojums, kas EVTI jāveic, ievērojot šā panta 7. punktu, neskar kompetentās iestādes atbildību steidzami nosūtīt sīku informāciju par būtisko ar IKT saistīto incidentu attiecīgajai iestādei uzņēmējā dalībvalstī, ja centrālajam vērtspapīru depozitārijam uzņēmējā dalībvalstī ir nozīmīga pārrobežu darbība, ja būtiskais ar IKT saistītais incidents, visticamāk, radīs smagas sekas uzņēmējas dalībvalsts finanšu tirgiem un ja starp kompetentajām iestādēm ir sadarbības mehānismi saistībā ar finanšu vienību uzraudzību.

20. pants

Ziņojumu satura un veidņu saskaņošana

EUI, ar Apvienotās komitejas starpniecību un apspriežoties ar *ENISA* un ECB, izstrādā:

a) kopējo regulatīvo tehnisko standartu projektus, ar ko:

   i) nosaka ziņojumu par būtiskiem ar IKT saistītiem incidentiem saturu, lai atspoguļotu 18. panta 1. punktā noteiktos kritērijus un ietvertu papildu elementus, piemēram, sīku informāciju nolūkā noteikt, vai iesniegtie ziņojumi ir relevanti citām dalībvalstīm, un to, vai tas ir vai nav būtisks ar maksājumiem saistīts darbības vai drošības incidents;

   ii) nosaka termiņus sākotnējam paziņojumam un katram 19. panta 4. punktā minētajam ziņojumam;

   iii) nosaka par būtiskiem kiberdraudiem veikto paziņojumu saturu.

   Izstrādājot minētos regulatīvo tehnisko standartu projektus, EUI ņem vērā finanšu vienības lielumu, tās pakalpojumu, darbību un operāciju veidu, apmēru un sarežģītību, kā arī tās vispārējo riska profilu, un jo īpaši nolūkā nodrošināt, ka šīs daļas a) punkta ii) apakšpunkta vajadzībām dažādi termiņi attiecīgā gadījumā varētu atspoguļot finanšu nozaru īpatnības, neskarot vienotas pieejas uzturēšanu ar IKT saistīto incidentu paziņošanai, ievērojot šo regulu un Direktīvu (ES) 2022/2555 EUI attiecīgā gadījumā sniedz pamatojumu, ja notiek novirzīšanās no pieejām, kas ieņemtas minētās direktīvas kontekstā;

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

EUI iesniedz Komisijai pirmās daļas a) punktā minēto kopējo regulatīvo tehnisko standartu projektus un pirmās daļas b) punktā minēto kopējo īstenošanas tehnisko standartu projektus līdz 2024. gada 17. jūlijam.

Komisijai tiek deleģētas pilnvaras papildināt šo regulu, pieņemot pirmās daļas a) punktā minētos kopējos regulatīvos tehniskos standartus saskaņā ar 10.–14. pantu Regulās (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010.

Komisijai tiek deleģētas pilnvaras pieņemt pirmās daļas b) punktā minētos kopējos īstenošanas tehniskos standartus saskaņā ar 15. pantu Regulās (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010.

21. 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. Kopīgajā 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 kopīgajā ziņojumā ir vismaz šādi elementi:

a) priekšnoteikumi šāda vienota ES centrmezgla izveidei;

b) ieguvumi, ierobežojumi un riski, tostarp riski, kas saistīti ar augstu sensitīvas informācijas koncentrāciju;

c) spēja, kas nepieciešama, lai nodrošinātu sadarbspēju salīdzinājumā ar citām attiecīgajām ziņošanas shēmām;

d) darbības vadības elementi;

e) dalības nosacījumi;

f) tehniskā kārtība, kādā finanšu vienības un valstu kompetentās iestādes var piekļūt vienotajam ES centrmezglam;

g) provizorisks novērtējums par finansiālajām izmaksām, kas radušās ar vienotā ES centrmezgla atbalsta darbības platformas izveidi, tostarp tai vajadzīgajām speciālām zināšanām.

3. EUI iesniedz 1. punktā minēto ziņojumu Eiropas Parlamentam, Padomei un Komisijai līdz 2025. gada 17. janvārim.

22. pants

Uzraudzības atgriezeniskā saite

1. Neskarot tehnisko informāciju, konsultācijas vai tiesiskās aizsardzības līdzekļus un turpmākos pasākumus, ko *CSIRT* attiecīgā gadījumā var īstenot saskaņā ar valsts tiesību aktiem, ievērojot Direktīvu (ES) 2022/2555, kompetentā iestāde, saņemot sākotnējo paziņojumu un katru ziņojumu, kā minēts 19. panta 4. punktā, apstiprina paziņojuma saņemšanu un var, ja iespējams, savlaicīgi sniegt relevantu un samērīgu atgriezenisko saiti vai augsta līmeņa norādījumus finanšu vienībai, jo īpaši, darot pieejamu jebkādu attiecīgu anonimizētu informāciju un izlūkdatus par līdzīgiem draudiem, un var apspriest tiesiskās aizsardzības līdzekļus, kas piemēroti finanšu vienības līmenī, un veidus, kā pēc iespējas samazināt un mīkstināt nelabvēlīgo ietekmi visā finanšu nozarē. Neskarot saņemto uzraudzības atgriezenisko saiti, finanšu vienības ir pilnībā atbildīgas par tādu ar IKT saistītu incidentu apstrādi, par kuriem ziņots, ievērojot 19. panta 1. punktu, un par šādu incidentu sekām.

2. EUI ar Apvienotās komitejas starpniecību katru gadu sniedz anonimizētu un apkopotu informāciju par būtiskiem ar IKT saistītiem incidentiem, par kuriem saskaņā ar 19. panta 6. punktu sīkas ziņas sniedz kompetentās iestādes, izklāstot vismaz būtisko ar IKT saistīto incidentu skaitu, to būtību un to ietekmi uz finanšu vienību vai klientu darbību, veiktos korektīvos pasākumus un radušās izmaksas.

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

23. pants

Ar maksājumiem saistīti darbības vai drošības incidenti, kas attiecas uz kredītiestādēm, maksājumu iestādēm, konta informācijas pakalpojumu sniedzējiem un elektroniskās naudas iestādēm

Šajā nodaļā paredzētās prasības piemēro arī ar maksājumiem saistītiem darbības vai drošības incidentiem un būtiskiem ar maksājumiem saistītiem darbības vai drošības incidentiem, ja tie attiecas uz kredītiestādēm, maksājumu iestādēm, konta informācijas pakalpojumu sniedzējiem un elektroniskās naudas iestādēm.

IV NODAĻA

Digitālās darbības noturības testēšana

24. pants

Vispārējās prasības digitālās darbības noturības testu veikšanai

1. Lai novērtētu gatavību apstrādāt ar IKT saistītus incidentus, identificēt vājās vietas, trūkumus un nepilnības digitālās darbības noturībā un nekavējoties īstenot korektīvos pasākumus, finanšu vienības, kas nav mikrouzņēmumi, ņemot vērā 4. panta 2. punktā izklāstītos kritērijus, izveido, uztur un pārskata stabilu un visaptverošu digitālās darbības noturības testēšanas programmu kā 6. pantā minētās IKT riska pārvaldības sistēmas neatņemamu daļu.

2. Digitālās darbības noturības testēšanas programma ietver virkni novērtējumu, testu, metožu, prakšu un rīku, ko piemēro saskaņā ar 25. un 26. pantu.

3. Veicot šā panta 1. punktā minēto digitālās darbības noturības testēšanas programmu, finanšu vienības, kas nav mikrouzņēmumi, ievēro uz risku balstītu pieeju, ņemot vērā 4. panta 2. punktā izklāstītos kritērijus, pienācīgi ņemot vērā IKT riska mainīgo ainu, jebkādus īpašus riskus, kuriem attiecīgā 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, kas nav mikrouzņēmumi, nodrošina, ka testēšanu veic neatkarīgas personas, kas var būt iekšējas vai ārējas. Ja testus veic iekšējais testētājs, finanšu vienības šā uzdevuma veikšanai piešķir pietiekamus resursus un nodrošina, ka visā testa izstrādes un izpildes laikā netiek pieļauti interešu konflikti.

5. Finanšu vienības, kas nav mikrouzņēmumi, izveido procedūras un politikas pasākumus, lai noteiktu par prioritārām, klasificētu un novērstu visas problēmas, kuru pastāvēšana ir atklāta 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, kas nav mikrouzņēmumi, nodrošina, ka vismaz reizi gadā pienācīgi tiek testētas visas IKT sistēmas un lietojumprogrammas, kas atbalsta kritiski svarīgas vai svarīgas funkcijas.

25. pants

IKT rīku un sistēmu testēšana

1. Regulas 24. pantā minētā digitālās darbības noturības testēšanas programma saskaņā ar 4. panta 2. punktā izklāstītajiem kritērijiem paredz tādu atbilstīgu testu veikšanu kā, piemēram, ievainojamības novērtējumi un skenēšana, atklātā pirmkoda analīze, tīkla drošības novērtējumi, nepilnību analīze, fiziskās drošības pārbaudes, anketas un skenēšanas programmatūras risinājumi, pirmkodu pārskatīšanas, ja iespējams, uz scenārijiem balstīti testi, saderības testēšana, veiktspējas testēšana, pilnīga testēšana (“no gala līdz galam”) un ielaušanās testēšana.

2. Centrālie vērtspapīru depozitāriji un centrālie darījumu partneri veic ievainojamības novērtējumu, pirms tiek ieviestas vai atkārtoti ieviestas jaunas vai esošas lietojumprogrammas un infrastruktūras komponenti, un IKT pakalpojumi, kas atbalsta finanšu vienības kritiski svarīgas vai svarīgas funkcijas.

3. Mikrouzņēmumi 1. punktā minētos testus veic, uz risku balstītu pieeju kombinējot ar IKT testēšanas stratēģisko plānošanu, pienācīgi ņemot vērā nepieciešamību saglabāt līdzsvarotu pieeju starp resursu mērogu un laiku, kas jāpiešķir šajā pantā paredzētajai IKT testēšanai, no vienas puses, un steidzamību, riska veidu, informācijas aktīvu un sniegto pakalpojumu kritisko svarīgumu, kā arī jebkādus citus relevantus faktorus, cita starpā finanšu vienības spēju uzņemties aprēķinātu risku, no otras puses.

26. pants

IKT rīku, sistēmu un procesu padziļināta testēšana, balstoties uz DVIT

1. Finanšu vienības, kas nav 16. panta 1. punkta pirmajā daļā minētās vienības un kas nav mikrouzņēmumi, kuri ir identificēti saskaņā ar šā panta 8. punkta trešo daļu, vismaz reizi trijos gados veic padziļinātu testēšanu, izmantojot DVIT. Pamatojoties uz finanšu vienības riska profilu un ņemot vērā operacionālos apstākļus, kompetentā iestāde vajadzības gadījumā var pieprasīt finanšu vienībai samazināt vai palielināt šo biežumu.

2. Katrs draudu vadīts ielaušanās tests aptver vairākas vai visas finanšu vienības kritiski svarīgās vai svarīgās funkcijas, un to veic aktīvā izstrādes sistēmā, kas atbalsta šīs funkcijas.

Finanšu vienības identificē visas attiecīgās pamatā esošās IKT sistēmas, procesus un tehnoloģijas, kas atbalsta kritiski svarīgas vai svarīgas funkcijas un IKT pakalpojumus, tostarp tos, kas atbalsta kritiski svarīgas vai svarīgas funkcijas, kas nodotas ārpakalpojumā vai par ko noslēgts līgums ar trešām personām, kas sniedz IKT pakalpojumus.

Finanšu vienības novērtē, kuras kritiski svarīgās vai svarīgās funkcijas ir jāiekļauj DVIT. Šā novērtējuma rezultāts nosaka precīzu DVIT jomu, un to validē kompetentās iestādes.

3. Ja DVIT joma aptver trešās personas, kas sniedz IKT pakalpojumus, finanšu vienība veic nepieciešamos pasākumus un aizsardzības pasākumus, lai nodrošinātu šādu trešo personu, kas sniedz IKT pakalpojumus, dalību DVIT, un nepārtraukti saglabā pilnīgu atbildību par to, lai tiktu nodrošināta atbilstība šai regulai.

4. Neskarot 2. punkta pirmo un otro daļu, – ja ir pamatoti sagaidāms, ka trešās personas, kas sniedz IKT pakalpojumus, 3. punktā minētajai dalībai DVIT būs nelabvēlīga ietekme uz to pakalpojumu kvalitāti vai drošību, kurus trešā persona, kas sniedz IKT pakalpojumus, sniedz klientiem, kas ir vienības, kuras neietilpst šīs regulas darbības jomā, vai uz to datu konfidencialitāti, kas saistīti ar šādiem pakalpojumiem, finanšu vienība un trešā persona, kas sniedz IKT pakalpojumus, var rakstiski vienoties par to, ka trešā persona, kas sniedz IKT pakalpojumus, tieši noslēdz līgumiskas vienošanās ar ārēju testētāju, lai vienas izraudzītas finanšu vienības vadībā veiktu apvienotu DVIT, kurā iesaistītas vairākas finanšu vienības (apvienotā testēšana), kurām trešā persona, kas sniedz IKT pakalpojumus, sniedz IKT pakalpojumus.

Minētā apvienotā testēšana aptver attiecīgo IKT pakalpojumu klāstu, ar kuriem atbalsta kritiski svarīgās vai svarīgās funkcijas, par kurām finanšu vienības ir noslēgušas līgumu ar attiecīgo trešo personu, kas sniedz IKT pakalpojumus. Apvienoto testēšanu uzskata par DVIT, ko veic finanšu vienības, kuras piedalās apvienotajā testēšanā.

To finanšu vienību skaitu, kas piedalās apvienotajā testēšanā, pienācīgi kalibrē, ņemot vērā iesaistīto pakalpojumu sarežģītību un veidus.

5. Finanšu vienības, sadarbojoties ar trešām personām, kas sniedz IKT pakalpojumus, un citām iesaistītajām pusēm, tostarp testētājiem, bet ne kompetentajām iestādēm, piemēro efektīvu riska pārvaldības kontroli, lai mazinātu riskus, ka varētu tikt ietekmēti pašas finanšu vienības, tās darījumu partneru vai finanšu nozares dati, bojāti aktīvi un traucētas kritiski svarīgas vai svarīgas funkcijas, pakalpojumi vai darbības.

6. Pēc testa beigām, kad apstiprināti ziņojumi un sanācijas plāni, finanšu vienība un attiecīgā gadījumā ārējie testētāji iesniedz iestādei, kas izraudzīta saskaņā ar 9. vai 10. punktu, attiecīgo konstatējumu kopsavilkumu, sanācijas plānus un dokumentus, kas apliecina, ka DVIT ir veikta atbilstīgi prasībām.

7. Iestādes finanšu vienībām sniedz apliecinājumu, kas apstiprina, ka tests tika veikts saskaņā ar prasībām, kā apliecināts dokumentos, lai starp kompetentajām iestādēm būtu iespējama draudu vadītu ielaušanās testu savstarpēja atzīšana. Finanšu vienība paziņo attiecīgajai kompetentajai iestādei par apliecinājumu, attiecīgo konstatējumu kopsavilkumu un sanācijas plānus.

Neskarot šādu apliecinājumu, finanšu vienības nepārtraukti ir pilnībā atbildīgas par 4. punktā minēto testu ietekmi.

8. Finanšu vienības slēdz līgumus ar testētājiem, lai veiktu DVIT saskaņā ar 27. pantu. Ja finanšu vienības DVIT veikšanas nolūkā izmanto iekšējos testētājus, tās katra trešā testa veikšanai slēdz līgumu ar ārēju testētāju.

Kredītiestādes, kas saskaņā ar Regulas (ES) Nr. 1024/2013 6. panta 4. punktu ir klasificētas kā nozīmīgas, saskaņā ar 27. panta 1. punkta a)–e) apakšpunktu izmanto tikai ārējos testētājus.

Kompetentās iestādes identificē finanšu vienības, kam ir pienākums veikt DVIT, ņemot vērā 4. panta 2. punktā izklāstītos kritērijus, pamatojoties uz šādu faktoru izvērtējumu:

a) ar ietekmi saistīti faktori, jo īpaši tas, kādā mērā finanšu vienības sniegtie pakalpojumi un veiktās darbības ietekmē finanšu nozari;

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

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

9. Dalībvalstis finanšu nozarē var izraudzīties vienotu publisku iestādi, lai tā valsts līmenī būtu atbildīga par jautājumiem, kuri saistīti ar DVIT finanšu nozarē, un šajā nolūkā tai uztic visas kompetences un uzdevumus.

10. Ja nav notikusi izraudzīšanās saskaņā ar šā panta 9. punktu un neskarot pilnvaras identificēt finanšu vienības, kam prasīts veikt DVIT, kompetentā iestāde dažu vai visu šajā pantā un 27. pantā minēto uzdevumu izpildi var deleģēt citai valsts iestādei finanšu nozarē.

11. EUI, vienojoties ar ECB, izstrādā kopēju regulatīvo tehnisko standartu projektu saskaņā ar *TIBER–EU* sistēmu, lai sīkāk precizētu:

a) 8. punkta otrās daļas piemērošanas vajadzībām izmantotos kritērijus;

b) prasības un standartus, kas reglamentē iekšējo testētāju izmantošanu;

c) prasības attiecībā uz:

   i) šā panta 2. punktā minēto DVIT darbības jomu;

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

   iii) testēšanas rezultātu, slēgšanas un kļūdu novēršanas posmus;

d) tādas uzraudzības un citas attiecīgas sadarbības veidu, kas vajadzīga, lai īstenotu DVIT un veicinātu minētās testēšanas savstarpēju atzīšanu saistībā ar finanšu vienībām, kas darbojas vairāk nekā vienā dalībvalstī, lai nodrošinātu pienācīgu uzraudzības iesaisti un elastīgu īstenošanu nolūkā ņemt vērā finanšu apakšnozaru vai vietējo finanšu tirgu īpatnības.

Izstrādājot minēto regulatīvo tehnisko standartu projektus, EUI pienācīgi ņem vērā visas īpašās iezīmes, kas izriet no darbību atšķirīgā rakstura dažādās finanšu pakalpojumu nozarēs.

Minētos regulatīvo tehnisko standartu projektus EUI iesniedz Komisijai līdz 2024. gada 17. jūlijam.

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

27. pants

Prasības testētājiem attiecībā uz DVIT veikšanu

1. Finanšu vienības DVIT veikšanai izmanto tikai testētājus:

a) kam ir visaugstākā piemērotība un reputācija;

b) kam ir tehniskās un organizēšanas spējas un kuri ir apliecinājuši, ka tiem ir īpaša zinātība par draudu izlūkdatiem, ielaušanās testēšanu un sarkanās komandas testēšanu;

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

d) kas sniedz neatkarīgu apliecinājumu vai revīzijas ziņojumu saistībā ar tādu risku stabilu pārvaldību, kas ir saistīti ar DVIT veikšanu, tostarp finanšu vienības konfidenciālās informācijas pienācīgu aizsardzību un finanšu vienības uzņēmējdarbības risku atlīdzināšanu;

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

2. Izmantojot iekšējos testētājus, finanšu iestādes nodrošina, ka papildus 1. punkta prasībām, tiek izpildīti šādi nosacījumi:

a) šādu izmantošanu ir apstiprinājusi attiecīgā kompetentā iestāde vai vienotā publiskā iestāde, kas izraudzīta saskaņā ar 26. panta 9. un 10. punktu;

b) attiecīgā kompetentā iestāde ir pārbaudījusi, ka finanšu vienībai ir pietiekami atvēlēti resursi, un nodrošinājusi, ka visā testa izstrādes un izpildes laikā netiek pieļauti interešu konflikti; un

c) draudu izlūkdatu sniedzējs ir ar finanšu vienību nesaistīts.

3. Finanšu vienības nodrošina, ka ar ārējiem testētājiem noslēgtajos līgumos ir obligāti noteikts stabili pārvaldīt DVIT rezultātus un ka jebkāda datu apstrāde, tostarp izveidošana, glabāšana, apkopošana, izstrāde, ziņošana, paziņošana vai iznīcināšana, nerada riskus finanšu vienībai.

V NODAĻA

Ar trešo personu saistīta IKT riska pārvaldība

I iedaļa

Ar trešo personu saistīta IKT riska stabilas pārvaldības pamatprincipi

28. pants

Vispārējie principi

1. Finanšu vienības savās IKT riska pārvaldības sistēmās, kā minēts 6. panta 1. punktā, pārvalda ar trešo personu saistīto IKT risku kā IKT riska neatņemamu daļu saskaņā ar turpmāk izklāstītajiem principiem:

a) finanšu vienības, kurām ir līgumiskas vienošanās par IKT pakalpojumu izmantošanu savas uzņēmējdarbības veikšanai, nepārtraukti ir pilnībā atbildīgas par visu šajā regulā un piemērojamos finanšu pakalpojumu tiesību aktos noteikto saistību ievērošanu un izpildi;

b) finanšu vienības īsteno ar trešo personu saistītā IKT riska pārvaldību saskaņā ar proporcionalitātes principu, ņemot vērā:

i) ar IKT saistītu atkarību veidu, apmēru, sarežģītību un svarīgumu;

ii) riskus, kuri rodas no tādas 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 pieejamību individuālā un grupas līmenī.

2. Finanšu vienības, kas nav 16. panta 1. punkta pirmajā daļā minētās vienības un kas nav mikrouzņēmumi, kā daļu no savas IKT riska pārvaldības sistēmas pieņem un regulāri pārskata ar trešo personu saistītā IKT riska stratēģiju, attiecīgā gadījumā ņemot vērā 6. panta 9. punktā minēto vairāku piegādātāju stratēģiju. Ar trešo personu saistītā IKT riska stratēģijā ietver rīcībpolitiku par tādu IKT pakalpojumu izmantošanu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, ko nodrošina trešās personas, kas sniedz IKT pakalpojumus, un to piemēro individuāli un attiecīgā gadījumā subkonsolidēti un konsolidēti. Vadības struktūra, pamatojoties uz finanšu vienības vispārējā riska profila un uzņēmējdarbības pakalpojumu apmēra un sarežģītības novērtējumu, regulāri pārskata apzinātos riskus attiecībā uz līgumiskajām vienošanām par tādu IKT pakalpojumu izmantošanu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas.

3. 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 IKT pakalpojumiem, ar ko atbalsta kritiski svarīgas vai svarīgas funkcijas, no tām, kas uz tiem neattiecas.

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

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

Finanšu vienības laikus informē kompetento iestādi par visām plānotajām līgumiskajām vienošanām par tādu IKT pakalpojumu izmantošanu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, kā arī par to, ka funkcija ir kļuvusi par kritiski svarīgu vai svarīgu.

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

a) novērtē, vai līgumiskā vienošanās attiecas uz tādu IKT pakalpojumu izmantošanu, ar kuriem atbalsta 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, kā minēts 29. pantā;

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.

5. Līgumiskas vienošanās ar trešām personām, kas sniedz IKT pakalpojumus, finanšu vienības var slēgt tikai tad, ja attiecīgo trešo personu darbība atbilst attiecīgiem informācijas drošības standartiem. Kad minētās līgumiskās vienošanās attiecas uz kritiski svarīgām vai svarīgām funkcijām, finanšu vienības pirms vienošanos noslēgšanas pienācīgi ņem vērā to, kā trešās personas, kas sniedz IKT pakalpojumus, izmanto visjaunākos un kvalitatīvākos informācijas drošības standartus.

6. Īstenojot piekļuves, pārbaudes un revīzijas tiesības attiecībā uz trešo personu, kas sniedz IKT pakalpojumus, finanšu vienības, pamatojoties 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 līgumiskas vienošanās, kas noslēgtas ar trešām personām, kas sniedz IKT pakalpojumus, par IKT pakalpojumu izmantošanu rada lielu tehnisku sarežģītību, finanšu vienība pārbauda, vai revidentiem – gan iekšējiem, gan ārējiem revidentiem, vai revidentu grupai – ir atbilstīgas prasmes un zināšanas, lai efektīvi veiktu attiecīgās revīzijas un novērtējumus.

7. Finanšu vienības nodrošina, ka līgumiskas vienošanās par IKT pakalpojumu izmantošanu var izbeigt jebkurā no šādiem gadījumiem:

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

b) pastāv 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 trešās personas, kas sniedz IKT pakalpojumus, pierādītas nepilnības attiecībā uz tās vispārējā IKT riska pārvaldību un jo īpaši attiecībā uz veidu, kādā tas nodrošina datu – gan personas, gan citādi sensitīvu datu, gan datu, kas nav personas dati – pieejamību, autentiskumu, integritāti un konfidenciālitāti;

d) ja kompetentā iestāde vairs nevar efektīvi uzraudzīt finanšu vienību attiecīgās līgumiskās vienošanās nosacījumu rezultātā vai ar to saistītu apstākļu dēļ.

8. Attiecībā uz IKT pakalpojumiem, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, finanšu vienības ievieš atkāpšanās stratēģijas. Atkāpšanās stratēģijās ņem vērā riskus, kas var rasties trešo personu, kas sniedz IKT pakalpojumus, līmenī, jo īpaši to saistību iespējamu neizpildi, sniegto IKT pakalpojumu kvalitātes pasliktināšanos, jebkādus uzņēmējdarbības traucējumus IKT pakalpojumu neatbilstīgas vai nesekmīgas sniegšanas dēļ vai jebkādu būtisku risku, kas rodas saistībā ar attiecīgā IKT pakalpojuma pienācīgu un nepārtrauktu izvēršanu, vai līgumiskas vienošanās izbeigšanu ar trešām personām, kas sniedz IKT pakalpojumus, jebkuru no 7. punktā minēto apstākļu dēļ.

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

a) netraucējot to uzņēmējdarbībai;

b) neierobežojot atbilstību regulatīvajām prasībām;

c) nekaitējot klientiem sniegto pakalpojumu nepārtrauktībai un kvalitātei.

Atkāpšanās plāni ir visaptveroši, dokumentēti un saskaņā ar 4. panta 2. punktā noteiktajiem kritērijiem tiek pietiekami pārbaudīti un periodiski pārskatīti.

Finanšu vienības identificē alternatīvus risinājumus un izstrādā pārejas plānus, kas tām ļauj ar līgumu noteiktos IKT pakalpojumus 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 pirmajā daļā minēto apstākļu gadījumā.

9. EUI ar Apvienotās komitejas starpniecību izstrādā īstenošanas tehnisko standartu projektus, lai izveidotu standarta veidnes 3. punktā minētā informācijas reģistra vajadzībām, tostarp informāciju, kas ir kopīga visām līgumiskajām vienošanām par IKT pakalpojumu izmantošanu. EUI iesniedz minētos īstenošanas tehnisko standartu projektus Komisijai līdz 2024. gada 17. janvārim.

Komisijai tiek deleģētas pilnvaras pieņemt pirmajā daļā minētos īstenošanas tehniskos standartus saskaņā ar 15. pantu Regulās (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010.

10. EUI ar Apvienotās komitejas starpniecību izstrādā regulatīvo tehnisko standartu projektus, lai sīkāk precizētu 2. punktā minētās rīcībpolitikas detalizēto saturu saistībā ar līgumisko vienošanos par tādu IKT pakalpojumu izmantošanu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, ko nodrošina trešās personas, kas sniedz IKT pakalpojumus.

Izstrādājot minēto regulatīvo tehnisko standartu projektus, EUI ņem vērā finanšu vienības lielumu un vispārējo riska profilu, kā arī tās pakalpojumu, darbību un darbību veidu, apmēru un sarežģītību. Minēto regulatīvo tehnisko standartu projektu EUI iesniedz Komisijai līdz 2024. gada 17. janvārim.

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

29. pants

IKT koncentrācijas riska sākotnējais novērtējums

1. Veicot 28. panta 4. punkta c) apakšpunktā minētā riska identificēšanu un novērtēšanu, finanšu vienības ņem vērā arī to, vai plānotā līgumiskas vienošanās noslēgšana par IKT pakalpojumiem, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, 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, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, sniegšanu ar to 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 uzņēmējdarbības vajadzībām un mērķiem.

2. Ja līgumiskās vienošanās par IKT pakalpojumu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, izmantošanu ietver iespēju, ka trešā persona, kas sniedz IKT pakalpojumus, IKT pakalpojumus, ar kuriem atbalsta kritiski svarīgu vai svarīgu funkciju, nodod tālāk apakšuzņēmējiem – citām trešām personām, kas sniedz IKT pakalpojumus, finanšu vienības izvērtē ieguvumus un riskus, kas varētu rasties saistībā ar šādu nodošanu apakšuzņēmējiem, jo īpaši, ja IKT apakšuzņēmējs ir iedibināts trešā valstī.

Ja līgumiskas vienošanās attiecas uz IKT pakalpojumiem, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, finanšu vienības pienācīgi ņem vērā maksātnespējas tiesību aktu noteikumus, ko piemērotu, ja trešā persona, kas sniedz IKT pakalpojumus, bankrotē, kā arī jebkādus ierobežojumus, kas varētu rasties saistībā ar finanšu vienības datu steidzamu atgūšanu.

Ja līgumisko vienošanos par IKT pakalpojumu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, izmantošanu slēdz ar trešo personu, kas sniedz IKT pakalpojumus un kas ir iedibināta trešā valstī, līdztekus pirmajā un otrajā daļā minētajiem apsvērumiem finanšu vienības apsver arī atbilstību Savienības datu aizsardzības noteikumiem un tiesību aktu efektīvu izpildi minētajā trešā valstī.

Ja līgumiskajās vienošanās par tādu IKT pakalpojumu izmantošanu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, paredz apakšuzņēmuma līgumu slēgšanu, 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.

30. pants

Svarīgākie līgumu noteikumi

1. Finanšu vienības un trešās personas, kas sniedz IKT pakalpojumus, tiesības un pienākumus sadala skaidri un noformulē rakstiski. Pilns līgums ietver pakalpojuma līmeņa vienošanās, un to dokumentē vienā rakstiskā dokumentā, kas pusēm ir pieejams papīra formātā, vai dokumentā, kam ir cits lejupielādējams, noturīgs un piekļūstams formāts.

2. Līgumiskas vienošanās par IKT pakalpojumu izmantošanu ietver vismaz šādus elementus:

a) skaidru un pilnīgu aprakstu par visām funkcijām un IKT pakalpojumiem, ko nodrošina trešā persona, kas sniedz IKT pakalpojumus, norādot, vai ir atļauts IKT pakalpojumu, ar ko atbalsta kritiski svarīgu vai svarīgu funkciju, vai būtiskas tā daļas nodot apakšuzņēmējam un, ja tā ir – nosacījumus, ko piemēro nodošanai apakšuzņēmējam;

b) ar līgumu vai apakšuzņēmuma līgumu nodoto funkciju un IKT pakalpojumu izpildes un datu apstrādes vietas, proti, reģioni vai valstis, tostarp to glabāšanas vietu, kā arī prasību trešai personai, kas sniedz IKT pakalpojumus, iepriekš paziņot finanšu vienībai, ja tā plāno šādas vietas mainīt;

c) noteikumus par pieejamību, autentiskumu, integritāti un konfidencialitāti, saistībā ar datu, tostarp personas datu, aizsardzību;

d) noteikumus par to, kā nodrošināt piekļuvi finanšu vienības apstrādātajiem personas datiem un datiem, kas nav personas dati, to atgūšanu un atgriešanu viegli piekļūstamā formātā trešās personas, kas sniedz IKT pakalpojumus, maksātnespējas, noregulējuma vai uzņēmējdarbības izbeigšanas gadījumā vai līgumisku vienošanos izbeigšanas gadījumā;

e) pakalpojumu līmeņa aprakstus, tostarp to atjauninājumus un labojumus;

f) trešās personas, kas sniedz IKT pakalpojumus, pienākumu sniegt palīdzību finanšu vienībai bez papildu izmaksām vai par izmaksām, kas ir noteiktas *ex-ante*, ja notiek IKT incidents, kas ir saistīts ar finanšu vienībai sniegto IKT pakalpojumu;

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

h) izbeigšanas tiesības un ar tām saistītos minimālos paziņošanas termiņus attiecībā uz līgumiskās vienošanās izbeigšanu atbilstoši tam, kā to sagaida kompetentās iestādes un noregulējuma iestādes;

i) nosacījumus trešo personu, kas sniedz IKT pakalpojumus, dalībai finanšu vienību IKT drošības izpratnes veidošanas programmās un digitālās darbības noturības mācībās saskaņā ar 13. panta 6. punktu.

3. Papildus 2. punktā minētajiem elementiem līgumiskās vienošanās par tādu IKT pakalpojumu izmantošanu, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas, ietver vismaz:

a) pilnīgus pakalpojumu līmeņa aprakstus, tostarp to atjauninājumus un labojumus, norādot precīzus kvantitatīvus un kvalitatīvus darbības mērķus saskaņotajos pakalpojumu līmeņos, lai ļautu finanšu vienībai efektīvi uzraudzīt IKT pakalpojumus un lai bez liekas kavēšanās varētu veikt atbilstīgus koriģējošus pasākumus, ja netiek ievēroti saskaņotie pakalpojumu līmeņi;

b) trešai personai, kas sniedz IKT pakalpojumus, saistošos paziņošanas termiņus un ziņošanas pienākumus attiecībā pret finanšu vienību, tostarp paziņošanu par jebkādu notikumu attīstību, kura varētu būtiski ietekmēt trešās personas, kas sniedz IKT pakalpojumus, spēju efektīvi sniegt IKT pakalpojumus, ar ko atbalsta kritiski svarīgas vai svarīgas funkcijas atbilstīgi saskaņotajiem pakalpojumu līmeņiem;

c) prasības trešai personai, kas sniedz IKT pakalpojumus, īstenot un testēt uzņēmējdarbības ārkārtas rīcības plānus un ieviest IKT drošības pasākumus, instrumentus un politikas pasākumus, kas nodrošina pienācīgu drošības līmeni finanšu vienības pakalpojumu sniegšanai saskaņā ar tās normatīvo regulējumu;

d) trešās personas, kas sniedz IKT pakalpojumus, pienākumu piedalīties un pilnībā sadarboties finanšu vienības DVIT, kā minēts 26. un 27. pantā;

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

i) finanšu vienības vai ieceltas trešās personas un kompetentās iestādes neierobežotas tiesības piekļūt, pārbaudīt un veikt revīziju, kā arī tiesības uz attiecīgo dokumentu kopēšanu uz vietas, ja tiem ir būtiski svarīga nozīme trešo personu, kas sniedz IKT pakalpojumus, darbībās, un šo tiesību 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) trešās personas, kas sniedz IKT pakalpojumus, pienākumu pilnībā sadarboties kompetento iestāžu, galvenā pārrauga, finanšu vienības vai ieceltas trešās personas veiktajās pārbaudēs uz vietas un revīzijās; un

iv) pienākumu sniegt sīku informāciju par šādu pārbaužu un revīziju tvērumu, procedūrām, kuras jāievēro, un biežumu;

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

i) kuras laikā trešā persona, kas sniedz IKT pakalpojumus, turpinās nodrošināt attiecīgās funkcijas vai IKT pakalpojumus nolūkā samazināt finanšu vienības darbības traucējumu risku vai nodrošināt tās efektīvu noregulējumu un pārstrukturēšanu;

ii) kas ļauj finanšu vienībai migrēt pie citas trešās personas, kas sniedz IKT pakalpojumus, vai pāriet uz iekšējiem risinājumiem, kas atbilst sniegtā pakalpojuma sarežģītībai.

Atkāpjoties no e) apakšpunkta, trešā persona, kas sniedz IKT pakalpojumus, un finanšu vienība, kas ir mikrouzņēmums, var vienoties, ka finanšu vienības piekļuves, pārbaudes un revīzijas veikšanas tiesības ir iespējams deleģēt neatkarīgai trešai personai, kuru iecēlusi trešā persona, kas sniedz IKT pakalpojumus, un ka finanšu vienība no šādas trešās personas jebkurā brīdī var pieprasīt informāciju un garantiju par izpildes rezultātu, kuru nodrošina trešā persona, kas sniedz IKT pakalpojumus.

4. Sarunās par līgumisku vienošanos finanšu vienības un trešās personas, kas sniedz IKT pakalpojumus, apsver iespēju izmantot līguma standartklauzulas, ko publiskās iestādes izstrādājušas attiecībā uz konkrētiem pakalpojumiem.

5. EUI ar Apvienotās komitejas starpniecību izstrādā regulatīvo tehnisko standartu projektus, lai sīkāk precizētu 2. punkta a) apakšpunktā minētos elementus, kas finanšu vienībai jānosaka un jānovērtē, slēdzot apakšuzņēmuma līgumus par IKT pakalpojumiem, ar kuriem atbalsta kritiski svarīgas vai svarīgas funkcijas.

Izstrādājot minēto regulatīvo tehnisko standartu projektus, EUI ņem vērā finanšu vienības lielumu un vispārējo riska profilu, kā arī tās pakalpojumu, darbību un operāciju veidu, apmēru un sarežģītību.

Minēto regulatīvo tehnisko standartu projektus EBI iesniedz Komisijai līdz 2024. gada 17. jūlijam.

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

II iedaļa

Kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, pārraudzības sistēma

31. pants

Kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, izraudzīšanās

1. EUI ar Apvienotās komitejas starpniecību un pēc saskaņā ar 32. panta 1. punktu izveidotā Pārraudzības foruma ieteikuma:

a) izraugās trešās personas, kas sniedz IKT pakalpojumus, kuras ir kritiski svarīgas finanšu vienībām, pēc novērtējuma, kurā ņemti vērā 2. punktā minētie kritēriji;

b) par galveno pārraugu katrai kritiski svarīgai trešai personai, kas sniedz IKT pakalpojumus, ieceļ EUI, kas saskaņā ar Regulām (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 vai (ES) Nr. 1095/2010 ir atbildīga par finanšu vienībām, kurām aktīvu kopējā vērtība veido lielāko daļu no visu to finanšu vienību kopējo aktīvu vērtības, kuras izmanto pakalpojumus, kurus sniedz attiecīgās kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, ko apliecina minēto finanšu vienību individuālo bilanču summa.

2. Šā panta 1. punkta a) apakšpunktā minētās izraudzīšanās pamatā ir visi turpmāk minētie kritēriji attiecībā uz IKT pakalpojumiem, ko sniedz trešā persona, kas sniedz IKT pakalpojumus:

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 finanšu vienību skaitu un to finanšu vienību aktīvu kopējo vērtību, kurām attiecīgā trešā persona, kas sniedz IKT pakalpojumus, sniedz 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) to globālo sistēmiski nozīmīgo iestāžu (G-SNI) vai citu sistēmiski nozīmīgu iestāžu (C-SNI) skaits, kuras 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, kas saistītas ar attiecīgo datu un darba slodzes daļēju vai pilnīgu migrēšanu no attiecīgās trešās personas, kas sniedz IKT pakalpojumus, pie citas trešās personas, kas sniedz IKT pakalpojumus, ko rada vai nu būtiskas finansiālās izmaksas, laika vai citu resursu patēriņš, ko varētu radīt migrācijas process, vai palielināts IKT risks vai citi operacionālie riski, kam finanšu vienība šādā migrēšanā varētu tikt pakļauta.

3. Ja trešā persona, kas sniedz IKT pakalpojumus, pieder pie grupas, 2. punktā minētos kritērijus ņem vērā saistībā ar IKT pakalpojumiem, ko sniedz grupa kopumā.

4. Kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus un ir daļa no grupas, izraugās vienu juridisku personu par koordinācijas punktu, lai nodrošinātu pienācīgu pārstāvību un saziņu ar galveno pārraugu.

5. Galvenais pārraugs paziņo trešai personai, kas sniedz IKT pakalpojumus, par novērtējuma rezultātiem, pēc kuriem notiek 1. punkta a) apakšpunktā minētā izraudzīšanās. Trešā persona, kas sniedz IKT pakalpojumus, sešu nedēļu laikā no paziņojuma dienas var iesniegt galvenajam pārraugam argumentētu paziņojumu ar visu būtisko informāciju novērtējuma vajadzībām. Galvenais pārraugs izskata argumentēto paziņojumu un var pieprasīt papildu informāciju, kas iesniedzama 30 kalendāro dienu laikā no šāda paziņojuma saņemšanas.

Pēc tam, kad trešā persona, kas sniedz IKT pakalpojumus, ir izraudzīta par kritiski svarīgu, EUI ar Apvienotās komitejas starpniecību paziņo trešai personai, kas sniedz IKT pakalpojumus, par šādu izraudzīšanu un par sākuma datumu, no kura uz to faktiski attieksies pārraudzības darbības. Minētais sākuma datums ir ne vēlāk kā vienu mēnesi pēc paziņojuma. Trešā persona, kas sniedz IKT pakalpojumus, paziņo finanšu vienībām, kurām tā sniedz pakalpojumus, par to, ka tā ir izraudzīta par kritiski svarīgu.

6. Komisija tiek pilnvarota līdz 2024. gada 17. jūlijam pieņemt deleģēto aktu saskaņā ar 57. pantu, lai papildinātu šo regulu, sīkāk precizējot šā panta 2. punktā minētos kritērijus.

7. Šā panta 1. punkta a) apakšpunktā minēto izraudzīšanu neizmanto, kamēr Komisija saskaņā ar 6. punktu nav pieņēmusi deleģēto aktu.

8. Šā panta 1. punkta a) apakšpunktā minēto izraudzīšanu nepiemēro:

i) finanšu vienībām, kas sniedz IKT pakalpojumus citām finanšu vienībām;

ii) trešām personām, kas sniedz IKT pakalpojumus un kurām piemēro Līguma par Eiropas Savienības darbību 127. panta 2. punktā minēto uzdevumu atbalstam izveidotās pārraudzības sistēmas;

iii) IKT pakalpojumu sniedzējiem, kas pieder vienai grupai;

iv) trešām personām, kas sniedz IKT pakalpojumus tikai vienā dalībvalstī finanšu vienībām, kuras darbojas tikai attiecīgajā dalībvalstī.

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

10. Šā panta 1. punkta a) apakšpunkta mērķiem kompetentās iestādes katru gadu apkopotā veidā nosūta 28. panta 3. punkta trešajā daļā minētos ziņojumus saskaņā ar 32. 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.

11. Trešās personas, kas sniedz IKT pakalpojumus un kuras nav iekļautas 9. punktā minētajā sarakstā, var pieprasīt, lai tās saskaņā ar 1. punkta a) apakšpunktu izraugās par kritiski svarīgām.

Pirmās daļas vajadzībām trešā persona, kas sniedz IKT pakalpojumus, iesniedz argumentētu pieteikumu EBI, EVTI vai EAAPI, kas ar Apvienotās komitejas starpniecību lemj, vai izraudzīties minēto trešo personu, kas sniedz IKT pakalpojumus, par kritiski svarīgu 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.

12. Finanšu vienības izmanto pakalpojumus, ko sniedz trešā valstī iedibināta trešā persona, kas sniedz IKT pakalpojumus un kas ir izraudzīta kā kritiski svarīga saskaņā ar 1. punkta a) apakšpunktu, ja minētā persona 12 mēnešu laikā no izraudzīšanas ir iedibinājusi meitasuzņēmumu Savienībā.

13. Šā panta 12. punktā minētā kritiski svarīgā trešā persona, kas sniedz IKT pakalpojumus, informē galveno pārraugu par visām izmaiņām Savienībā iedibinātā meitasuzņēmuma vadības struktūrā.

32. pants

Pārraudzības sistēmas struktūra

1. Apvienotā komiteja saskaņā ar 57. panta 1. punktu Regulās (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010 izveido Pārraudzības forumu kā apakškomiteju, lai tā atbalstītu 31. panta 1. punkta b) apakšpunktā minēto Apvienotās komitejas un galvenā pārrauga darbību ar trešām personām saistīta IKT riska jomā visās finanšu nozarēs. Pārraudzības forums izstrādā Apvienotās komitejas kopīgās nostājas projektus un kopīgo aktu projektus šajā jomā.

Pārraudzības forums regulāri apspriež attiecīgās norises saistībā ar IKT risku un ievainojamību un veicina saskaņotas pieejas izmantošanu, uzraugot ar trešām personām saistīto IKT risku Savienības līmenī.

2. Pārraudzības forums katru gadu veic attiecībā uz visām kritiski svarīgajām trešām personām, 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 56. panta 1. punktu Regulās (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010 iesniedz visaptverošus kritiski svarīgo trešo personu, kas sniedz IKT pakalpojumus, kritērijus, ko Apvienotā komiteja pieņem kā EUI kopīgās nostājas.

4. Pārraudzības forumu veido:

a) EUI vadītāji;

b) viens augsta līmeņa pārstāvis no attiecīgās 46. pantā minētās kompetentās iestādes pašreizējā personāla katrā dalībvalstī;

c) katras EUI izpilddirektori un pa vienam pārstāvim no Komisijas, ESRK, ECB un *ENISA* kā novērotāji;

d) attiecīgā gadījumā – vēl viens 46. pantā minētās kompetentās iestādes pārstāvis no katras dalībvalsts kā novērotājs;

e) attiecīgā gadījumā – kā novērotājs viens tādu kompetento iestāžu pārstāvis, kas izraudzītas vai izveidotas saskaņā ar Direktīvu (ES) 2022/2555 un ir atbildīgas par tādas būtiskas vai svarīgas vienības uzraudzību, kas ir izraudzīta par kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, uz kuru attiecas minētā direktīva.

Pārraudzības forums attiecīgā gadījumā var vērsties pēc padoma pie neatkarīgiem ekspertiem, kas iecelti saskaņā ar 6. punktu.

5. Katra dalībvalsts izraugās attiecīgo kompetento iestādi, kuras personāla loceklis ir 4. punkta pirmās daļas b) apakšpunktā minētais augsta līmeņa pārstāvis, un par to informē galveno pārraugu.

EUI savā tīmekļa vietnē publicē sarakstu ar dalībvalstu izraudzītiem augsta līmeņa pārstāvjiem no attiecīgās kompetentās iestādes pašreizējā personāla.

6. Neatkarīgos ekspertus, kas minēti 4. punkta otrajā daļā, ieceļ Pārraudzības forums no ekspertu kopuma, kas atlasīti pēc publiska un pārredzama pieteikšanās procesa.

Neatkarīgos ekspertus ieceļ, pamatojoties uz viņu speciālajām zināšanām finansiālās stabilitātes, digitālās darbības noturības un IKT drošības jautājumos. Viņi rīkojas neatkarīgi un objektīvi vienīgi Savienības interesēs kopumā un nelūdz, un nepieņem Savienības iestāžu vai struktūru, jebkuras dalībvalsts valdības vai citas valsts vai privātas struktūras norādījumus.

7. EUI saskaņā ar 16. pantu Regulās (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010 līdz 2024. gada 17. jūlijam izdod pamatnostādnes par EUI un kompetento iestāžu sadarbību šīs iedaļas vajadzībām, kurās izklāstītas detalizētas procedūras un nosacījumi attiecībā uz uzdevumu sadali un izpildi starp kompetentajām iestādēm un EUI, un ziņas par informācijas apmaiņu, kas kompetentajām iestādēm nepieciešama, lai nodrošinātu turpmāku rīcību pēc ieteikumiem, kuri saskaņā ar 35. panta 1. punkta d) apakšpunktu adresēti kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus.

8. Šajā iedaļā izklāstītās prasības neskar Direktīvas (ES) 2022/2555 un citu Savienības noteikumu par mākoņdatošanas pakalpojumu sniedzēju pārraudzību piemērošanu.

9. 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.

33. pants

Galvenā pārrauga uzdevumi

1. Galvenais pārraugs, kurš iecelts saskaņā ar 31. panta 1. punkta b) apakšpunktu, veic norīkoto kritiski svarīgo trešo personu, kas sniedz IKT pakalpojumus, pārraudzību, un visos jautājumos, kas saistīti ar pārraudzību, ir galvenais kontaktpunkts minētajām trešām personām, kas sniedz IKT pakalpojumus.

2. Šā panta 1. punkta nolūkos 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 risku, ko tā var radīt finanšu vienībām.

Pirmajā daļā minētajā novērtējumā galvenā uzmanība tiek pievērsta IKT pakalpojumiem, ko sniedz tā kritiski svarīgā trešā persona, kas sniedz IKT pakalpojumus un kura atbalsta kritiski svarīgās vai svarīgās finanšu vienību funkcijas. Ja tas ir nepieciešams, lai pievērstos visiem attiecīgajiem riskiem, minētais novērtējums tiek attiecināts arī uz IKT pakalpojumiem, kas atbalsta funkcijas, kas nav tikai kritiski svarīgas vai svarīgas.

3. Šā panta 2. punktā minētais novērtējums ietver:

a) IKT prasības, kuru mērķis jo īpaši ir nodrošināt 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 datu pieejamības, autentiskuma, integritātes vai konfidencialitātes standartus;

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

c) riska pārvaldības procesus, tostarp IKT riska pārvaldības rīcībpolitiku, IKT darbības nepārtrauktības politiku un IKT reaģēšanas un 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 būtisku 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.

4. Pamatojoties uz 2. punktā minēto novērtējumu un koordinācijā ar 34. panta 1. punktā minēto Kopīgo pārraudzības tīklu (*JON*), galvenais pārraugs attiecībā uz katru kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, pieņem skaidru, detalizētu un pamatotu individuālo pārraudzības plānu, kurā aprakstīti ikgadējie pārraudzības mērķi un plānotās galvenās pārraudzības darbības. Šo plānu katru gadu paziņo kritiski svarīgajai trešai personai, kas sniedz IKT pakalpojumus.

Pirms pārraudzības plāna pieņemšanas galvenais pārraugs kritiski svarīgajai trešai personai, kas sniedz IKT pakalpojumus, paziņo pārraudzības plāna projektu.

Saņēmusi pārraudzības plāna projektu, kritiski svarīgā trešā persona, kas sniedz IKT pakalpojumus, 15 kalendāro dienu laikā var iesniegt argumentētu paziņojumu, kurā pamatoti izklāstītas gaidāmās sekas klientiem, kas ir vienības, kuras neietilpst šīs regulas darbības jomā, un attiecīgā gadījumā formulēti risinājumi risku mazināšanai.

5. Tiklīdz 4. punktā minētie gada pārraudzības plāni ir pieņemti un paziņoti kritiski svarīgajām trešām personām, kas sniedz IKT pakalpojumus, kompetentās iestādes attiecībā uz šādām kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, var veikt pasākumus tikai ar galvenā pārrauga piekrišanu.

34. pants

Darbības koordinācija starp galvenajiem pārraugiem

1. Lai nodrošinātu konsekventu pieeju pārraudzības darbībām un lai būtu iespējamas koordinētas vispārējas pārraudzības stratēģijas un saskaņotas darbības pieejas un darba metodika, trīs galvenie pārraugi, kuri iecelti saskaņā ar 31. panta 1. punkta b) apakšpunktu, izveido *JON*, lai veiktu savstarpēju koordināciju sagatavošanās posmos un lai koordinētu pārraudzības darbību veikšanu pār to attiecīgajām pārraugāmajām kritiski svarīgajām trešām personām, kas sniedz IKT pakalpojumus, kā arī jebkuras rīcības gaitā, kas var būt nepieciešama, ievērojot 42. pantu.

2. Šā panta 1. punkta nolūkos galvenie pārraugi izstrādā kopīgu pārraudzības protokolu, kurā norādītas detalizētas procedūras, kas jāievēro, veicot ikdienas koordināciju un lai nodrošinātu raitu apmaiņu un reaģēšanu. Protokolu periodiski pārskata, lai atspoguļotu darbības vajadzības, jo īpaši izmaiņas pārraudzības praktiskajā kārtībā.

3. Galvenie pārraugi *ad hoc* kārtībā var vērsties pēc tehniskām konsultācijām pie ECB un *ENISA*, dalīties praktiskā pieredzē vai piedalīties konkrētās *JON* koordinācijas sanāksmēs.

35. pants

Galvenā pārrauga pilnvaras

1. Pildot šajā iedaļā paredzētos pienākumus, galvenajam pārraugam ir šādas pilnvaras attiecībā uz kritiski svarīgajām trešām personām, kas sniedz IKT pakalpojumus:

a) pieprasīt visu attiecīgo informāciju un dokumentus saskaņā ar 37. pantu;

b) veikt vispārēju izmeklēšanu un pārbaudes saskaņā ar attiecīgi 38. un 39. pantu;

c) pēc pārraudzības darbību pabeigšanas pieprasīt ziņojumus, 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 33. panta 3. 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, tostarp 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 samazināšanu līdz minimumam;

   iii) jebkādiem plānotiem apakšuzņēmuma līgumiem, attiecībā uz kuriem galvenais pārraugs, pamatojoties uz tādas informācijas izskatīšanu, kas savākta saskaņā ar 37. un 38. pantu, uzskata, ka tālāka apakšuzņēmuma līguma slēgšana, tostarp tādi apakšuzņēmuma līgumi, ko kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, plāno slēgt ar citām trešām personām, kas sniedz IKT pakalpojumus, vai ar trešā valstī iedibinātiem IKT apakšuzņēmējiem, var radīt risku finanšu vienības pakalpojumu sniegšanai vai finanšu stabilitātes risku;

   iv) tālāku apakšuzņēmuma līgumu neslēgšanu, ja pastāv šādi kumulatīvi nosacījumi:

      — paredzētais apakšuzņēmējs ir trešā valstī iedibināta trešā persona, kas sniedz IKT pakalpojumus, vai trešā valstī iedibināts IKT apakšuzņēmējs,

      — apakšuzņēmuma līguma slēgšana attiecas uz kritiski svarīgu vai svarīgu finanšu vienības funkciju; un

— galvenais pārraugs uzskata, ka šādas apakšuzņēmuma līguma slēgšanas izmantošana rada nepārprotamu un nopietnu risku Savienības finanšu stabilitātei vai finanšu vienībām, tostarp finanšu vienību spējai izpildīt uzraudzības prasības.

Šā apakšpunkta iv) punkta nolūkos trešās personas, kas sniedz IKT pakalpojumus, izmantojot 41. panta 1. punkta b) apakšpunktā minēto veidni, nosūta informāciju par apakšuzņēmuma līguma slēgšanu galvenajam pārraugam.

2. Īstenojot šajā pantā minētās pilnvaras, galvenais pārraugs:

a) nodrošina regulāru koordināciju *JON* ietvaros un jo īpaši attiecīgos gadījumos cenšas panākt konsekventas pieejas attiecībā uz kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, pārraudzību;

b) pienācīgi ņem vērā satvaru, kas izveidots ar Direktīvu (ES) 2022/2555, un vajadzības gadījumā apspriežas ar attiecīgajām kompetentajām iestādēm, kas izraudzītas vai izveidotas saskaņā ar minēto direktīvu, lai izvairītos no tādu tehnisko un organizatorisko pasākumu dublēšanās, kas, ievērojot minēto direktīvu, varētu attiekties uz kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus;

c) ciktāl iespējams, cenšas līdz minimumam samazināt risku, ka tiek traucēti kritiski svarīgo trešo personu sniegtie IKT pakalpojumi klientiem, kas ir vienības, kuras neietilpst šīs regulas darbības jomā.

3. Pirms 1. punktā minēto pilnvaru īstenošanas galvenais pārraugs apspriežas ar Pārraudzības forumu.

Pirms sniegt ieteikumus saskaņā ar 1. punkta d) apakšpunktu, galvenais pārraugs dod iespēju trešai personai, kas sniedz IKT pakalpojumus, 30 kalendāro dienu laikā sniegt attiecīgu informāciju, kurā pamatoti izklāstītas gaidāmās sekas klientiem, kas ir vienības, kuras neietilpst šīs regulas darbības jomā, un attiecīgā gadījumā formulēti risinājumi risku mazināšanai.

4. Galvenais pārraugs informē *JON* par 1. punkta a) un b) apakšpunktā minēto pilnvaru īstenošanas rezultātiem. Galvenais pārraugs bez nepamatotas kavēšanās 1. punkta c) apakšpunktā minētos ziņojumus nosūta *JON* un to finanšu vienību kompetentajām iestādēm, kuras izmanto attiecīgās kritiski svarīgās trešās personas sniegtos IKT pakalpojumus.

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

6. Gadījumā, ja pilnībā vai daļēji netiek veikti pasākumi, kurus ir noteikts pienākums veikt, ievērojot saskaņā ar 1. punkta a), b) un c) apakšpunktā paredzēto pilnvaru īstenošanu, un pēc tam, kad ir pagājušas vismaz 30 kalendārās dienas no dienas, kurā kritiski svarīgā trešā persona, kas sniedz IKT pakalpojumus, saņēma paziņojumu par attiecīgajiem pasākumiem, galvenais pārraugs pieņem lēmumu, ar ko piemēro periodisku soda maksājumu, lai piespiestu kritiski svarīgo trešo personu, kas sniedz IKT pakalpojumus, ievērot minētos pasākumus.

7. Šā panta 6. punktā minēto periodisko soda maksājumu piemēro katru dienu, līdz tiek panākta atbilstības prasību ievērošana, un ne ilgāk kā sešus mēnešus pēc tam, kad par lēmumu piemērot periodisku soda maksājumu ir paziņots kritiski svarīgajai trešai personai, kas sniedz IKT pakalpojumus.

8. Periodiskā soda maksājuma summa, rēķinot no lēmumā par periodiska soda maksājuma piemērošanu paredzētā datuma, nepārsniedz 1 % no kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, dienas vidējā apgrozījuma pasaulē iepriekšējā finanšu gadā. Nosakot soda maksājuma lielumu, galvenais pārraugs ņem vērā šādus kritērijus attiecībā uz neatbilstību 6. punktā minētajiem pasākumiem:

a) neatbilstības smagums un ilgums;

b) tas, vai neatbilstība ir notikusi tīši vai nolaidības dēļ;

c) apmērs, kādā trešā persona, kas sniedz IKT pakalpojumus, ir sadarbojusies ar galveno pārraugu.

Pirmās daļas nolūkos, lai panāktu konsekventu pieeju, galvenais pārraugs iesaistās apspriedēs *JON* ietvaros.

9. 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.

10. Galvenais pārraugs publisko informāciju par visiem piemērotajiem periodiskajiem soda maksājumiem, ja vien šādas informācijas publiskošana būtiski nekaitē finanšu tirgiem vai nerada nesamērīgu kaitējumu iesaistītajām personām.

11. Galvenais pārraugs pirms periodiska soda maksājuma piemērošanas saskaņā ar 6. punktu nodrošina procesā iesaistītās 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. Procesā iesaistītā kritiski svarīgā trešā persona, kas sniedz IKT pakalpojumus, ir tiesīga 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.

36. pants

Galvenā pārrauga pilnvaru īstenošana ārpus Savienības

1. Ja pārraudzības mērķus nevar sasniegt, mijiedarbojoties ar 31. panta 12. punkta nolūkā izveidoto meitasuzņēmuma struktūru vai īstenojot pārraudzības darbības Savienībā esošās telpās, galvenais pārraugs var īstenot pilnvaras, kas minētas turpmāk minētajos noteikumos, jebkādās telpās, kas atrodas trešā valstī un kas pieder kritiski svarīgai trešai persona, kas sniedz IKT pakalpojumus, vai ko tā izmanto jebkādā veidā pakalpojumu sniegšanai Savienības finanšu vienībām, saistībā ar tās uzņēmējdarbību, funkcijām vai pakalpojumiem, tostarp jebkādos administratīvajos, darījumu vai darbības birojos, telpās, zemēs, ēkās vai citos īpašumos:

a) 35. panta 1. punkta a) apakšpunktā; un

b) 35. panta 1. punkta b) apakšpunktā saskaņā ar 38. panta 2. punkta a), b) un d) apakšpunktu un 39. panta 1. punktā un 2. punkta a) apakšpunktā.

Pirmajā daļā minētās pilnvaras var īstenot, ievērojot visus turpmāk minētos nosacījumus:

i) galvenais pārraugs pārbaudes veikšanu trešā valstī uzskata par nepieciešamu, lai varētu pilnīgi un efektīvi veikt savus šajā regulā paredzētos pienākumus;

ii) pārbaude trešā valstī ir tieši saistīta ar IKT pakalpojumu sniegšanu finanšu vienībām Savienībā;

iii) attiecīgā kritiski svarīgā trešā persona, kas sniedz IKT pakalpojumus, piekrīt pārbaudes veikšanai trešā valstī; un

iv) galvenais pārraugs ir oficiāli informējis attiecīgās trešās valsts attiecīgo iestādi, un tā nav pret to cēlusi nekādus iebildumus.

2. Neskarot Savienības iestāžu un dalībvalstu attiecīgo kompetenci, 1. punkta nolūkos EBI, EVTI vai EAAPI noslēdz administratīvās sadarbības vienošanās ar trešās valsts attiecīgo iestādi, lai galvenais pārraugs un tā izraudzītā darba grupa nosūtījumam attiecīgajā trešajā valstī varētu raiti veikt pārbaudes minētajā trešā valstī. Minētās sadarbības vienošanās nerada juridiskas saistības attiecībā uz Savienību un tās dalībvalstīm, nedz arī liedz dalībvalstīm un to kompetentajām iestādēm slēgt divpusējas vai daudzpusējas vienošanās ar minētajām trešām valstīm un to attiecīgajām iestādēm.

Minētajās sadarbības vienošanās norāda vismaz šādus elementus:

a) koordinācijas procedūras attiecībā uz pārraudzības darbībām, ko veic saskaņā ar šo regulu, un jebkādu analogu pārraudzību attiecībā uz IKT trešo personu risku finanšu nozarē, kuru īsteno attiecīgās trešās valsts attiecīgā iestāde, tostarp informāciju par to, kā tiek nosūtīta minētās iestādes piekrišana tam, ka galvenais pārraugs un tā izraudzītā darba grupa iestādes jurisdikcijā esošajā teritorijā veic vispārēju izmeklēšanu un pārbaudes uz vietas, kā minēts 1. punkta pirmajā daļā;

b) mehānisms, saskaņā ar kuru tiek nosūtīta visa nozīmīgā informācija starp EBI, EVTI vai EAAPI un attiecīgās trešās valsts attiecīgo iestādi, jo īpaši saistībā ar informāciju, ko var pieprasīt galvenais pārraugs, ievērojot 37. pantu;

c) mehānisms, saskaņā ar kuru attiecīgās trešās valsts attiecīgā iestāde ātri informē EBI, EVTI vai EAAPI par gadījumiem, kad ir uzskatāms, ka trešā valstī iedibināta trešā persona, kas sniedz IKT pakalpojumus un kas ir izraudzīta kā kritiski svarīga saskaņā ar 31. panta 1. punkta a) apakšpunktu, ir pārkāpusi prasības, kuras tai ir pienākums ievērot saskaņā ar attiecīgās trešās valsts spēkā esošajiem tiesību aktiem, kad tiek sniegti pakalpojumi finanšu vienībām minētajā trešajā valstī, kā arī par piemērotajiem tiesiskās aizsardzības līdzekļiem un sodiem;

d) regulāra aktuālās informācijas nosūtīšana par norisēm saistībā ar regulējumu un uzraudzību attiecībā uz finanšu iestāžu ar trešo personu saistītā IKT riska uzraudzību attiecīgajā trešā valstī;

e) informācija par to, ka vajadzības gadījumā tiek atļauta attiecīgās trešās valsts iestādes pārstāvja piedalīšanās pārbaudēs, ko veic galvenais pārraugs un izraudzītā darba grupa.

3. Ja galvenais pārraugs nespēj veikt 1. un 2. punktā minētās pārraudzības darbības ārpus Savienības, galvenais pārraugs:

a) īsteno savas 35. pantā paredzētās pilnvaras, pamatojoties uz visiem tam pieejamajiem faktiem un dokumentiem;

b) dokumentē un skaidro visas sekas, kādas rada tā nespēja veikt paredzētās pārraudzības darbības, kā minēts šajā pantā.

Šā punkta b) apakšpunktā minētās iespējamās sekas tiek ņemtas vērā galvenā pārrauga ieteikumos, ko izdod, ievērojot 35. panta 1. punkta d) apakšpunktu.

37. 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, tostarp visus attiecīgos uzņēmējdarbības vai darbības dokumentus, līgumus, rīcībpolitikas, dokumentāciju, 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 informācija, pārstāvi, ka tā var nesniegt šo informāciju, bet, ja tā atbildi sniedz brīvprātīgi, sniegtā informācija nedrīkst būt nepatiesa un maldinoša.

3. Ar lēmumu 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 35. panta 6. punktā paredzēto periodisko soda maksājumu, ja pieprasītā informācija nav sniegta pilnā apmērā vai ja šāda informācija netiek sniegta šā punkta d) apakšpunktā minētajā termiņā;

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

4. Pieprasīto informāciju sniedz kritiski svarīgo trešo personu, kas sniedz IKT pakalpojumus, pārstāvji. 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 par informācijas sniegšanu kopiju to finanšu vienību kompetentajām iestādēm, kuras izmanto attiecīgo kritiski svarīgo trešo personu, kas sniedz IKT pakalpojumus, sniegtos pakalpojumus, un JON.

38. pants

Vispārēja izmeklēšana

1. Lai veiktu savus pienākumus saskaņā ar šo regulu, galvenais pārraugs, kam palīdz 40. panta 1. punktā minētā kopīgā pārbaudes grupa, vajadzības gadījumā var veikt izmeklēšanu par kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus.

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) noņemt vai iegūt šādu uzskaites dokumentu, datu, dokumentētu procedūru un jebkādu citu materiālu apstiprinātas kopijas vai izrakstus;

c) izsaukt kritiski svarīgās 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 35. panta 6. punktā paredzētos periodiskos soda maksājumus, ja pieprasīto uzskaites dokumentu, datu, dokumentētu procedūru vai citu materiālu sagatavošana vai atbilžu sniegšana uz trešās personas, kas sniedz IKT pakalpojumus, pārstāvjiem uzdotajiem jautājumiem nenotiek vai ir nepilnīga.

4. Kritiski svarīgo 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 35. panta 6. punktā, tiesiskās aizsardzības līdzekļus, kuri pieejami saskaņā ar Regulām (ES) Nr. 1093/2010, (ES) Nr. 1094/2010 un (ES) Nr. 1095/2010, un tiesības vērsties Tiesā, lai šo lēmumu pārskatītu.

5. Pirms izmeklēšanas sākuma galvenais pārraugs laicīgi informē to finanšu vienību kompetentās iestādes, kas izmanto IKT pakalpojumus, ko sniedz šī kritiski svarīgā trešā persona, kas sniedz IKT pakalpojumus, par paredzēto izmeklēšanu un atļauju saņēmušo personu identitāti.

Galvenais pārraugs paziņo *JON* visu informāciju, kas nodota saskaņā ar pirmo daļu.

39. pants

Pārbaudes

1. Lai veiktu savus pienākumus saskaņā ar šo regulu, galvenais pārraugs, kam palīdz 40. panta 1. punktā minētās kopīgās 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.

Lai īstenotu pirmajā daļā minētās pilnvaras, galvenais pārraugs apspriežas ar *JON*.

2. Amatpersonas un citas personas, kuras galvenais pārraugs pilnvarojis veikt pārbaudi uz vietas, ir tiesīgas:

a) iekļūt jebkurās šādās uzņēmuma telpās, zemes gabalos vai īpašumā; un

b) aizzīmogot jebkuras šāda uzņēmuma telpas, uzskaites žurnālus un reģistrus uz tik ilgu laiku un tādā apjomā, kāds vajadzīgs pārbaudei.

Amatpersonas un citas personas, kuras galvenais pārraugs pilnvarojis, īsteno savas pilnvaras, uzrādot rakstisku atļauju, kurā norādīts pārbaudes priekšmets un mērķis, kā arī 35. panta 6. punktā paredzētie periodiskie soda maksājumi gadījumam, ja attiecīgo kritiski svarīgo trešo personu, kas sniedz IKT pakalpojumus, pārstāvji nepakļaujas pārbaudei.

3. Pirms pārbaudes sākuma galvenais pārraugs laicīgi informē to finanšu vienību kompetentās iestādes, kas izmanto IKT pakalpojumus, ko sniedz minētā trešā persona.

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

5. Pirms jebkādas plānotas pārbaudes uz vietas galvenais pārraugs 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 pārbaude sāksies, un norāda periodiskos soda maksājumus, kas paredzēti 35. panta 6. punktā, tiesiskās aizsardzības līdzekļus, kas pieejami saskaņā ar Regulām (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 trešo personu, kas sniedz IKT pakalpojumus, par šāda iebilduma sekām, tostarp par iespēju attiecīgo finanšu vienību kompetentajām iestādēm prasīt finanšu vienībām izbeigt ar minēto kritiski svarīgo trešo personu, kas sniedz IKT pakalpojumus, noslēgtās līgumiskās vienošanās.

40. pants

Pastāvīgā pārraudzība

1. Veicot pārraudzības darbības, jo īpaši vispārēju izmeklēšanu vai pārbaudes, galvenajam pārraugam palīdz katrai kritiski svarīgajai trešai personai, kas sniedz IKT pakalpojumus, izveidota kopīga pārbaudes grupa.

2. Šā panta 1. punktā minētās kopīgās pārbaudes grupas sastāvā ir darbinieki no:

a) EUI;

b) attiecīgajām kompetentajām iestādēm, kas uzrauga finanšu vienības, kurām IKT pakalpojumus sniedz kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus;

c) valsts kompetentās iestādes, kas minēta 32. panta 4. punkta e) apakšpunktā, – brīvprātīgā kārtā;

d) vienas valsts kompetentās iestādes dalībvalstī, kurā ir iedibināta kritiski svarīgā trešā persona, kas sniedz IKT pakalpojumus, – brīvprātīgā kārtā.

Kopīgās pārbaudes grupas dalībniekiem ir zināšanas IKT jautājumos un operacionālā riska jomā. Kopīgā pārbaudes grupa strādā iecelta galvenā pārrauga darbinieka ("galvenā pārrauga koordinators") vadībā.

3. Trīs mēnešu laikā pēc tam, kad pabeigta izmeklēšana vai pārbaude, galvenais pārraugs, apspriedies ar Pārraudzības forumu, pieņem ieteikumus, ko saskaņā ar 35. pantā minētajām pilnvarām adresē kritiski svarīgajai trešai personai, kas sniedz IKT pakalpojumus.

4. Šā panta 3. punktā minētos ieteikumus nekavējoties paziņo kritiski svarīgajai trešai personai, kas sniedz IKT pakalpojumus, un to finanšu vienību kompetentajām iestādēm, kurām tas sniedz IKT pakalpojumus.

Lai izpildītu pārraudzības darbības, galvenais pārraugs 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.

41. pants

Saskaņoti nosacījumi, kas ļauj veikt pārraudzības darbības

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

a) informāciju, kas trešai personai, kas sniedz IKT pakalpojumus, jāsniedz pieteikumā ar brīvprātīgu pieprasījumu izraudzīšanai par kritiski svarīgu saskaņā ar par 31. panta 11. punktu;

b) tās informācijas saturu, struktūru un formātu, kas trešai personai, kas sniedz IKT pakalpojumus, jāiesniedz, jāatklāj vai jāpaziņo saskaņā ar 35. panta 1. punktu, tostarp veidni informācijas sniegšanai par apakšuzņēmuma līgumiem;

c) kritērijus, pēc kuriem nosaka kopīgās pārbaudes grupas sastāvu, nodrošinot EUI un attiecīgo kompetento iestāžu darbinieku līdzsvarotu dalību, viņu iecelšanu, uzdevumus un darba procedūras;

d) detalizētu informāciju par kompetento iestāžu veikto novērtējumu attiecībā uz pasākumiem, ko veic kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, pamatojoties uz galvenā pārrauga ieteikumiem saskaņā ar 42. panta 3. punktu.

2. Minēto regulatīvo tehnisko standartu projektu EUI iesniedz Komisijai līdz 2024. gada 17. jūlijam.

Komisijai tiek deleģētas pilnvaras papildināt šo regulu, pieņemot 1. punktā minētos regulatīvos tehniskos standartus saskaņā ar 10.–14. pantu Regulās (ES) Nr. 1093/2010, (ES) Nr. 1095/2010 un (ES) Nr. 1094/2010.

42. pants

Kompetento iestāžu turpmākā rīcība

1. 60 kalendāro dienu laikā pēc galvenā pārrauga sniegto ieteikumu saņemšanas saskaņā ar 35. panta 1. punkta d) apakšpunktu kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, vai nu informē galveno pārraugu par savu nodomu ievērot ieteikumus, vai sniedz pamatotu paskaidrojumu par minēto ieteikumu neievērošanu. Galvenais pārraugs nekavējoties nosūta šo informāciju attiecīgo finanšu vienību kompetentajām iestādēm.

2. Galvenais pārraugs publisko informāciju, ja kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, neinformē galveno pārraugu saskaņā ar 1. punktu vai ja kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, sniegtais skaidrojums netiek uzskatīts par pietiekamu. Publicētajā informācijā atklāj kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, identitāti, kā arī informāciju par neatbilstības veidu un būtību. Šāda informācija attiecas tikai uz to, kas ir būtisks un samērīgs, lai nodrošinātu sabiedrības informētību, izņemot gadījumus, kad šāda publicēšana radītu nesamērīgu kaitējumu iesaistītajām pusēm vai varētu nopietni apdraudēt finanšu tirgu pienācīgu darbību un integritāti vai visas Savienības finanšu sistēmas vai tās daļas stabilitāti.

Galvenais pārraugs informē trešo personu, kas sniedz IKT pakalpojumus, par šādu publiskošanu.

3. Kompetentās iestādes informē attiecīgās finanšu vienības par riskiem, kas identificēti kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, adresētajos ieteikumos saskaņā ar 35. panta 1. punkta d) apakšpunktu.

Pārvaldot ar trešo personu saistītu IKT risku, finanšu vienības ņem vērā pirmajā daļā minētos riskus.

4. Ja kompetentā iestāde uzskata, ka finanšu vienība ar trešo personu saistīta IKT riska pārvaldībā neņem vērā vai pietiekami nenovērš ieteikumos apzinātos konkrētos riskus, tā paziņo finanšu vienībai par iespēju 60 kalendāro dienu laikā pēc šāda paziņojuma saņemšanas, ievērojot 6. punktu, pieņemt lēmumu, ja nav atbilstīgu līgumisku vienošanos, kuru mērķis ir novērst šādus riskus.

5. Pēc 35. panta 1. punkta c) apakšpunktā minēto ziņojumu saņemšanas un pirms šā panta 6. punktā minētā lēmuma pieņemšanas kompetentās iestādes var brīvprātīgi apspriesties ar kompetentajām iestādēm, kas izraudzītas vai izveidotas saskaņā ar Direktīvu (ES) 2022/2555 un kas ir atbildīgas par tādas būtiskas vai svarīgas vienības uzraudzību, kura ir izraudzīta par kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, uz kuru attiecas minētā direktīva.

6. Kompetentās iestādes kā galējo līdzekli pēc paziņojuma saņemšanas un attiecīgā gadījumā pēc apspriešanās, kā izklāstīts šā panta 4. un 5. punktā, saskaņā ar 50. 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 līgumiskās vienošanās, kas ir noslēgtas ar kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus.

7. Ja kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, atsakās apstiprināt ieteikumus, pamatojoties uz pieeju, kas atšķiras no tās, kuru iesaka galvenais pārraugs, un šāda atšķirīga pieeja var negatīvi ietekmēt lielu skaitu finanšu vienību vai ievērojamu finanšu nozares daļu, un kompetento iestāžu atsevišķi brīdinājumi nav devuši konsekventu pieeju, lai mazinātu iespējamo risku finanšu stabilitātei, galvenais pārraugs pēc apspriešanās ar Pārraudzības forumu var kompetentajām iestādēm sniegt nesaistošus un nepubliskus atzinumus, lai vajadzības gadījumā veicinātu konsekventus un saskaņotus pārraudzības pēcpasākumus.

8. Pēc 35. panta 1. punkta c) apakšpunktā minēto ziņojumu saņemšanas kompetentās iestādes, pieņemot šā panta 6. punktā minēto lēmumu, 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 smagums un ilgums;

b) vai neatbilstība ir atklājusi būtiskus trūkumus kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, procedūrās, pārvaldības sistēmās, 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;

e) vai līgumisku vienošanos apturēšana vai izbeigšana rada risku finanšu vienības uzņēmējdarbības nepārtrauktībai, neskarot finanšu vienības centienus izvairīties no traucējumiem tā pakalpojumu sniegšanā;

f) attiecīgā gadījumā – atzinums, ko sniedz kompetentās iestādes, kas izraudzītas vai izveidotas saskaņā ar Direktīvu (ES) 2022/2555 un ir atbildīgas par tādas būtiskas vai svarīgas vienības uzraudzību, kura ir izraudzīta par kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, uz kuru attiecas minētā direktīva un kas ir pieprasīts brīvprātīgi saskaņā ar šā panta 5. punktu.

Kompetentās iestādes piešķir finanšu vienībām nepieciešamo laiku, lai tās varētu pielāgot līgumiskās vienošanās ar kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, lai izvairītos no negatīvas ietekmes uz to digitālās darbības noturību un ļautu tām izmantot atkāpšanās stratēģijas un pārejas plānus, kā minēts 28. pantā.

9. Šā panta 6. punktā minēto lēmumu paziņo 32. panta 4. punkta a), b) un c) apakšpunktā minētajiem Pārraudzības foruma dalībniekiem un *JON*.

Kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, kuras skar 6. punktā paredzētie lēmumi, pilnībā sadarbojas ar ietekmētajām finanšu vienībām, jo īpaši saistībā ar to līgumisko vienošanos apturēšanas vai izbeigšanas procesu.

10. Kompetentās iestādes regulāri informē galveno pārraugu par pieejām un pasākumiem, ko tās veikušas, pildot finanšu vienību uzraudzības uzdevumus, kā arī par līgumiskajām vienošanām, ko noslēgušas finanšu vienības, ja kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, nav daļēji vai pilnībā apstiprinājušas galvenā pārrauga tām adresētos ieteikumus.

11. Galvenais pārraugs pēc pieprasījuma var sniegt papildu skaidrojumus par sniegtajiem ieteikumiem, lai palīdzētu kompetentajām iestādēm veikt turpmākus pasākumus.

43. pants

Pārraudzības maksas

1. Galvenais pārraugs saskaņā ar šā panta 2. punktā minēto deleģēto aktu iekasē no kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, maksas, kas pilnībā sedz galvenā pārrauga nepieciešamos izdevumus saistībā ar pārraudzības uzdevumu veikšanu saskaņā ar šo regulu, tostarp visu to izmaksu atlīdzināšanu, kas var rasties 40. pantā minētās kopīgās pārbaudes grupas veiktā darba rezultātā, kā arī izmaksas par konsultācijām, ko sniedz neatkarīgie eksperti, kā minēts 32. panta 4. punkta otrajā daļā, saistībā ar jautājumiem, kas ir tiešās pārraudzības darbību jomā.

Kritiski svarīgai trešai personai, kas sniedz IKT pakalpojumus, piemērotās maksas sedz visas izmaksas, kas izriet no šajā iedaļā izklāstīto pienākumu izpildes, un ir proporcionālas tā apgrozījumam.

2. Komisija tiek pilnvarota līdz 2024. gada 17. jūlijam pieņemt deleģēto aktu saskaņā ar 57. pantu, lai papildinātu šo regulu, nosakot maksas apmēru un tās samaksas veidu.

44. pants

Starptautiska sadarbība

1. Neskarot 36. pantu, EBI, EVTI un EAAPI attiecīgi saskaņā ar 33. pantu Regulās (ES) Nr. 1093/2010, (ES) Nr. 1095/2010 un (ES) Nr. 1094/2010 var noslēgt administratīvas vienošanās ar trešo valstu regulatīvajām un uzraudzības iestādēm, lai veicinātu starptautisku sadarbību ar trešo personu saistītā IKT riska jomā 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 un iekšējā tirgus darbību.

VI NODAĻA

Informācijas apmaiņas kārtība

45. pants

Kiberdraudu informācijas un izlūkdatu informācijas apmaiņas kārtība

1. Finanšu vienības var savstarpēji apmainīties ar informāciju par kiberdraudiem un izlūkdatiem, tostarp 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 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 saskaņā ar Regulu (ES) 2016/679 un nostādnes par konkurences politiku.

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, par trešo personu, kas sniedz IKT pakalpojumus, iesaistīšanos un 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

46. pants

Kompetentās iestādes

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

a) kredītiestādēm un iestādēm, kam piemēro izņēmumu, ievērojot Direktīvu 2013/36/ES, – kompetentā iestāde, kas norīkota saskaņā ar minētās direktīvas 4. pantu, un kredītiestādēm, kas klasificētas kā nozīmīgas saskaņā ar Regulas (ES) Nr. 1024/2013 6. panta 4. punktu, – ECB saskaņā ar pilnvarām un uzdevumiem, kas piešķirti ar minēto regulu;

b) maksājumu iestādēm, tostarp maksājumu iestādēm, kam piemēro izņēmumu saskaņā ar Direktīvu (ES) 2015/2366, elektroniskās naudas iestādēm, tostarp tām, kam piemēro izņēmumu saskaņā ar Direktīvu 2009/110/EK, un konta informācijas pakalpojumu sniedzējiem, kas minēti 33. panta 1. punktā Direktīvā (ES) 2015/2366 – kompetentā iestāde, kas norīkota saskaņā ar 22. pantu Direktīvā (ES) 2015/2366;

c) ieguldījumu brokeru sabiedrībām – kompetentā iestāde, kas norīkota saskaņā ar Eiropas Parlamenta un Padomes Direktīvas (ES) 2019/2034 ([38]) 4. pantu;

d) kriptoaktīvu pakalpojumu sniedzējiem, kas saņēmuši atļauju saskaņā ar Regulu par kriptovalūtu tirgiem, un aktīviem piesaistītu žetonu emitentiem – kompetentā iestāde, kas norīkota saskaņā ar minētās regulas attiecīgo noteikumu;

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

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

g) tirdzniecības vietām un datu ziņošanas pakalpojumu sniedzējiem – kompetentā iestāde, kas norīkota saskaņā ar Direktīvas 2014/65/ES 67. pantu, un kompetentā iestāde, kā definēts Regulas (ES) Nr. 600/2014 2. panta 1. punkta 18) apakšpunktā;

h) darījumu reģistriem – kompetentā iestāde, kas norīkota saskaņā ar Regulas (ES) Nr. 648/2012 22. pantu;

i) alternatīvo ieguldījumu fondu pārvaldniekiem – kompetentā iestāde, kas norīkota saskaņā ar Direktīvas 2011/61/ES 44. pantu;

j) pārvaldības sabiedrībām – kompetentā iestāde, kas norīkota saskaņā ar Direktīvas 2009/65/EK 97. pantu;

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

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

m) arodpensijas kapitāla uzkrāšanas institūcijām – kompetentā iestāde, kas norīkota saskaņā ar Direktīvas (ES) 2016/2341 47. pantu;

n) kredītreitingu aģentūrām – kompetentā iestāde, kas norīkota saskaņā ar Direktīvas (EK) Nr. 1060/2009 21. pantu;

o) kritiski svarīgu etalonu administratoriem – kompetentā iestāde, kas norīkota saskaņā ar Regulas (ES) 2016/1011 40. un 41. pantu;

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

p) kolektīvās finansēšanas pakalpojumu sniedzējiem – kompetentā iestāde, kas norīkota saskaņā ar Regulas (ES) 2020/1503 29. pantu;

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

47. pants

Sadarbība ar struktūrām un iestādēm, kas izveidotas ar Direktīvu (ES) 2022/2555

1. Lai veicinātu sadarbību un nodrošinātu pārraudzības apmaiņu starp kompetentajām iestādēm, kas izraudzītas saskaņā ar šo regulu, un sadarbības grupu, kas izveidota ar Direktīvas (ES) 2022/2555 14. pantu, EUI un kompetentās iestādes var piedalīties sadarbības grupas darbībās, kas attiecas uz to pārraudzības darbībām attiecībā uz finanšu vienībām. EUI un kompetentās iestādes var lūgt, lai tās uzaicina piedalīties sadarbības grupas darbībās, kas saistītas ar būtiskām vai svarīgām vienībām, uz kurām attiecas Direktīva (ES) 2022/2555 un kuras arī ir izraudzītas par kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, ievērojot šīs regulas 31. pantu.

2. Attiecīgā gadījumā kompetentās iestādes var apspriesties un dalīties informācijā ar vienotajiem kontaktpunktiem un *CSIRT*, kas izraudzītas vai izveidotas saskaņā ar Direktīvu (ES) 2022/2555.

3. Attiecīgā gadījumā kompetentās iestādes var pieprasīt jebkādas attiecīgas tehniskas konsultācijas un palīdzību no kompetentajām iestādēm, kas izraudzītas vai izveidotas saskaņā ar Direktīvu (ES) 2022/2555, un izveidot sadarbības kārtību, lai varētu izveidot efektīvus un ātrus koordinācijas mehānismus.

4. Šā panta 3. punktā minētajos pasākumos cita starpā var precizēt procedūras uzraudzības un pārraudzības darbību koordinēšanai attiecībā uz būtiskām vai svarīgām vienībām, kuras, ievērojot šīs regulas 31. pantu, ir izraudzītas par kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus un uz kurām attiecas Direktīva (ES) 2022/2555, tostarp attiecībā uz izmeklēšanas un pārbaužu uz vietas veikšanu saskaņā ar valsts tiesību aktiem, kā arī mehānismiem informācijas apmaiņai starp kompetentajām iestādēm saskaņā ar šo regulu un tām kompetentajām iestādēm, kas izraudzītas vai izveidotas saskaņā ar minēto direktīvu, kas ietver piekļuvi informācijai, ko pieprasa pēdējās minētās iestādes.

48. pants

Iestāžu sadarbība

1. Kompetentās iestādes cieši sadarbojas savā starpā un attiecīgā gadījumā ar galveno pārraugu.

2. Kompetentās iestādes un galvenais pārraugs laikus savstarpēji apmainās ar visu attiecīgo informāciju par kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, kura tiem ir vajadzīga, lai veiktu savus attiecīgos pienākumus saskaņā ar šo regulu, jo īpaši attiecībā uz identificētajiem riskiem, pieejām un pasākumiem, kas veikti kā daļa no galvenā pārrauga pārraudzības uzdevumiem.

49. pants

Finanšu starpnozaru mācības, saziņa un sadarbība

1. EUI ar Apvienotās komitejas starpniecību un sadarbībā ar kompetentajām iestādēm, noregulējuma iestādēm, kā minēts Direktīvas 2014/59/ES 3. pantā, ECB, Vienoto noregulējuma valdi attiecībā uz informāciju par vienībām, uz kurām attiecas Regula (ES) Nr. 806/2014, ESRK un *ENISA*, attiecīgi, var izveidot mehānismus, kas ļauj apmainīties ar efektīvu praksi starp finanšu nozarēm, lai uzlabotu situācijas apzināšanos un apzinātu kopēju kiberievainojamību un riskus dažādās nozarēs.

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

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

2. Kompetentās iestādes, EUI un ECB cieši sadarbojas savā starpā un apmainās ar informāciju, lai veiktu savus pienākumus saskaņā ar 47.–54. pantu. Tās 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.

50. 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 savu pienākumu veikšanā, un saņemt vai noņemt to kopiju;

b) veikt pārbaudes vai izmeklēšanu uz vietas, tostarp, bet ne tikai:

   i) uzaicināt finanšu vienību pārstāvjus sniegt mutiskus vai rakstiskus paskaidrojumus par faktiem vai dokumentiem, kas attiecas uz izmeklēšanas priekšmetu un mērķi, un fiksēt atbildes;

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

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

3. Neskarot dalībvalstu tiesības piemērot krimināLsodus saskaņā ar 52. 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, ar ko pieprasa fiziskai vai juridiskai personai pārtraukt rīcību, kas ir pretrunā šai regulai, un atturēties no šādas rīcības 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; un

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

5. Ja 2. punkta c) apakšpunkts un 4. punkts attiecas uz juridiskām personām, dalībvalstis piešķir kompetentajām iestādēm pilnvaras, ievērojot valsts tiesību aktos paredzētos nosacījumus, 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 piemēro 2. punkta c) apakšpunktā minētos administratīvos sodus vai korektīvos pasākumus, ir pienācīgi pamatots un ka to var pārsūdzēt.

51. pants

Administratīvo sodu un korektīvo pasākumu piemērošanas pilnvaru īstenošana

1. Kompetentās iestādes pēc vajadzības īsteno pilnvaras uzlikt 50. pantā minētos administratīvos sodus un korektīvos pasākumus saskaņā ar attiecīgās valsts tiesisko regulējumu attiecīgā gadījumā šādi:

a) tieši;

b) sadarbojoties ar citām iestādēm;

c) uz savu atbildību deleģējot savas pilnvaras citām iestādēm; vai

d) iesniedzot pieteikumu kompetentajām tiesas iestādēm.

2. Kompetentās iestādes, nosakot saskaņā ar 50. 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 attiecīgos apstākļus, tostarp attiecīgā gadījumā šādus:

a) pārkāpuma būtiskumu, smagumu un ilgumu;

b) par pārkāpumu atbildīgās fiziskās vai juridiskās personas 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 fiziskās vai juridiskās personas sadarbības līmeni ar kompetento iestādi, neskarot vajadzību nodrošināt attiecīgās fiziskās vai juridiskās personas gūto ienākumu vai novērsto zaudējumu atdošanu;

g) atbildīgās fiziskās vai juridiskās personas iepriekš izdarītos pārkāpumus.

52. pants

Krimināls odi

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

2. Ja dalībvalstis izvēlējušās noteikt krimināls odus 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 krimināl izmeklēšanu 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.

53. pants

Ziņošanas pienākums

Dalībvalstis līdz 2025. gada 17. janvārim Komisijai, EVTI, EBI un EAAPI dara zināmus tos normatīvos un administratīvos aktus, ar kuriem tiek īstenotas šīs nodaļas prasības, tostarp jebkādas attiecīgās krimināltiesību normas. Dalībvalstis bez liekas kavēšanās informē Komisiju, EVTI, EBI un EAAPI par turpmākiem grozījumiem tajos.

54. 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, novērtējusi katru gadījumu atsevišķi, uzskata, ka identitātes publicēšana juridisku personu gadījumā vai identitātes un personas datu publicēšana fizisko personu gadījumā būtu nesamērīga, tostarp radītu riskus saistībā ar personas datu aizsardzību, apdraudētu finanšu tirgu stabilitāti vai notiekošu kriminālizmeklēšanu vai, ciktāl to var noteikt, radītu nesamērīgu kaitējumu iesaistītajai personai, tā attiecībā uz lēmumu, ar ko uzliek administratīvo sodu, pieņem vienu no šādiem risinājumiem:

a) atlikt tā publicēšanu, kamēr nav beiguši pastāvēt visi nepublicēšanas iemesli;

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

c) atturēties no publicēšanas, ja uzskata, ka ar a) un b) apakšpunktā izklāstītajiem risinājumiem nepietiek, lai garantētu, ka finanšu tirgu stabilitātei draudu nav, vai arī 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 ko uzliek administratīvu sodu, kurš ir pārsūdzēts attiecīgajās tiesu iestādēs, kompetentās iestādes nekavējoties savā oficiālajā tīmekļa vietnē ievieto arī šo informāciju un vēlāk – jebkādu vēlāku ar to saistītu informāciju par šādas pārsūdzības iznākumu. Publicē arī jebkuru tiesas nolēmumu, ar ko atceļ lēmumu par administratīvā soda uzlikšanu.

6. Kompetentās iestādes nodrošina, lai jebkura publikācija, kas minēta 1.–4. punktā, tās oficiālajā tīmekļa vietnē būtu pieejama tikai tik ilgi, cik tas ir nepieciešams šā panta piemērošanai. Šis laikposms nepārsniedz piecus gadus pēc tās publicēšanas.

55. 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, ievērojot šo regulu, nodarbina vai ir nodarbinājušas 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, tostarp informācijas apmaiņu starp kompetentajām iestādēm saskaņā ar šo regulu un tām kompetentajām iestādēm, kas izraudzītas vai izveidotas saskaņā ar Direktīvu (ES) 2022/2555, neatklāj nevienai citai personai vai iestādei citādi, nekā ir paredzēts Savienības vai valsts tiesību noteikumos;

4. Visu informāciju, ar ko kompetentās iestādes apmainās, ievērojot šo regulu, un kas attiecas uz darījumu vai darbības apstākļiem un citiem ekonomiskiem vai personiskiem 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.

56. pants

Datu aizsardzība

1. EUI un kompetentajām iestādēm ir atļauts apstrādāt personas datus tikai tad, ja tas ir nepieciešams, lai tās, ievērojot šo regulu, pildītu savus attiecīgos pienākumus un uzdevumus, jo īpaši veiktu izmeklēšanu, pārbaudi, informācijas pieprasījumu, paziņošanu, publicēšanu, izvērtēšanu, verifikāciju, novērtēšanu un pārraudzības plānu izstrādi. Personas datus apstrādā saskaņā ar Regulu (ES) 2016/679 vai Regulu (ES) 2018/1725, atkarībā no tā, kura ir piemērojama.

2. Ja vien citos nozares tiesību aktos nav noteikts citādi, 1. punktā minētos personas datus glabā līdz piemērojamo uzraudzības pienākumu izpildei un jebkurā gadījumā ne ilgāk kā 15 gadus, izņemot gadījumus, kad notiek tiesvedība, kuras vajadzībām šādi dati jāglabā ilgāk.

VIII NODAĻA

Deleģētie akti

57. pants

Deleģēšanas īstenošana

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

2. Pilnvaras pieņemt 31. panta 6. punktā un 43. panta 2. punktā minētos deleģētos aktus Komisijai piešķir uz piecu gadu laikposmu no 2024. gada 17. janvāra. Komisija sagatavo ziņojumu par pilnvaru deleģēšanu vēlākais deviņus mēnešus pirms piecu gadu laikposma beigām. Pilnvaru deleģēšana tiek automātiski pagarināta uz tāda paša ilguma laikposmiem, ja vien Eiropas Parlaments vai Padome neiebilst pret šādu pagarinājumu vēlākais trīs mēnešus pirms katra laikposma beigām.

3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 31. panta 6. punktā un 43. 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 katras dalībvalsts ieceltajiem ekspertiem saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu.

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

6. Saskaņā ar 31. panta 6. punktu un 43. panta 2. punktu pieņemts deleģētais akts stājas spēkā tikai tad, ja trijos 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 trim mēnešiem.

IX NODAĻA

Pārejas un nobeiguma noteikumi

I iedaļa

58. pants

Pārskatīšanas klauzula

1. Komisija līdz 2028. gada 17. janvārim pēc apspriešanās ar, attiecīgi, EUI un ESRK, veic pārskatīšanu un iesniedz ziņojumu Eiropas Parlamentam un Padomei, vajadzības gadījumā pievienojot tiesību akta priekšlikumu. Pārskatīšanā ir iekļauti vismaz šādi elementi:

a) kritēriji, kas paredzēti, lai saskaņā ar 31. panta 2. punktu izraudzītos kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus;

b) 19. pantā minēto būtisko kiberdraudu paziņošanas brīvprātīgums;

c) 31. panta 12. punktā minētā kārtība un galvenā pārrauga pilnvaras, kas paredzētas 35. panta 1. punkta d) apakšpunkta iv) punkta pirmajā ievilkumā, nolūkā novērtēt, cik efektīvi ir minētie noteikumi, lai nodrošinātu efektīvu pārraudzību pār trešā valstī iedibinātām kritiski svarīgām trešām personām, kas sniedz IKT pakalpojumus, un to, vai ir jāiedibina meitasuzņēmums Savienībā.

   Šā apakšpunkta pirmās daļas vajadzībām pārskatīšanā iekļauj 31. panta 12. punktā minētās kārtības analīzi, tostarp noteikumus par Savienības finanšu vienību piekļuvi no trešām valstīm sniegtiem pakalpojumiem un šādu pakalpojumu pieejamību Savienības tirgū, un tajā ņem vērā turpmākās norises to pakalpojumu tirgos, uz kuriem attiecas šī regula, finanšu vienību un finanšu uzraudzības iestāžu praktisko pieredzi minētās kārtības piemērošanā un attiecīgi minētās kārtības uzraudzībā, kā arī visas attiecīgās regulatīvās un uzraudzības norises starptautiskā līmenī.

d) tas, vai ir lietderīgi šīs regulas darbības jomā iekļaut 2. panta 3. punkta e) apakšpunktā minētās finanšu vienības, kas izmanto automatizētas pārdošanas sistēmas, ņemot vērā turpmākās tirgus norises šādu sistēmu izmantošanā;

e) kopīgā pārraudzības tīkla (*JON*) darbība un efektivitāte, pārraudzības sistēmā sekmējot pārraudzības konsekvenci un informācijas apmaiņas efektivitāti.

2. Saistībā ar Direktīvas (ES) 2015/2366 pārskatīšanu Komisija novērtē to, vai ir jāpalielina maksājumu sistēmu un maksājumu apstrādes darbību kibernoturība, un to, cik lietderīgi ir paplašināt šīs regulas darbības jomu, iekļaujot tajā maksājumu sistēmu operatorus un maksājumu apstrādes darbībās iesaistītās vienības. Ņemot vērā šo novērtējumu, Komisija Direktīvas (ES) 2015/2366 pārskatīšanas ietvaros iesniedz ziņojumu Eiropas Parlamentam un Padomei ne vēlāk kā 2023. gada 17. jūlijā.

Pamatojoties uz minēto pārskata ziņojumu un apspriedusies ar EUI, ECB un ESRK, Komisija attiecīgā gadījumā un kā daļu no tiesību akta priekšlikuma, ko tā var pieņemt, ievērojot Direktīvas (ES) 2015/2366 108. panta otro daļu, var iesniegt priekšlikumu nodrošināt, lai visiem maksājumu sistēmu operatoriem un maksājumu apstrādes darbībās iesaistītajām vienībām tiktu piemērota pienācīga pārraudzība, vienlaikus ņemot vērā jau pastāvošu centrālās bankas pārraudzību.

3. Komisija līdz 2026. gada 17. janvārim, apspriedusies ar EUI un Eiropas Revīzijas pārraudzības struktūru komiteju, veic pārskatīšanu un iesniedz ziņojumu Eiropas Parlamentam un Padomei, vajadzības gadījumā tam pievienojot tiesību akta priekšlikumu, par to, cik lietderīgi ir noteikt stingrākas prasības obligātajiem revidentiem un revīzijas uzņēmumiem attiecībā uz digitālās darbības noturību, iekļaujot obligātos revidentus un revīzijas uzņēmumus šīs regulas darbības jomā vai veicot grozījumus Eiropas Parlamenta un Padomes Direktīvā 2006/43/EK ([39]).

II iedaļa

Grozījumi

59. pants

Grozījumi Regulā (EK) Nr. 1060/2009

Regulu (EK) Nr. 1060/2009 groza šādi:

1) regulas I pielikuma A iedaļas 4. punkta 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) 2022/2554 (*).

_____

(*) Eiropas Parlamenta un Padomes Regula (ES) 2022/2554 (2022. gada 14. decembris) par finanšu sektora digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011 (OV L 333, 27.12.2022, p. 1.. lpp.).";

2) regulas III pielikuma 12. punktu aizstāj ar šādu:

"12. Kredītreitingu aģentūra pārkāpj 6. panta 2. punktu, to lasot saistībā ar I pielikuma A iedaļas 4. punktu, jo aģentūrai nav pareizu administratīvo vai grāmatvedības procedūru, iekšējo kontroles mehānismu, efektīvu riska novērtēšanas procedūru vai efektīvu kontroles pasākumu vai aizsargpasākumu IKT sistēmu pārvaldībai saskaņā ar Regulu (ES) 2022/2554; vai ja tā neīsteno vai neuztur lēmumu pieņemšanas procedūras vai organizatoriskās struktūras, kā noteikts minētajā punktā."

60. 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, tostarp IKT sistēmas, ko pārvalda saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2022/2554 (*).

_____

(*) Eiropas Parlamenta un Padomes Regula (ES) 2022/2554 (2022. gada 14. decembris) par finanšu sektora digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011 (OV L 333, 27.12.2022, 1.. lpp.).";

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

b) panta 6. punktu svītro;

2) regulas 34. pantu groza šādi:

a) panta 1. punktu aizstāj ar šādu:

"1. *CCP* izveido, īsteno un uztur piemērotu uzņēmējdarbības nepārtrauktības politiku un negadījuma seku novēršanas plānu, kurā iekļauj saskaņā ar Regulu (ES) 2022/2554 ieviestu un īstenotu IKT uzņēmējdarbības nepārtrauktības politiku un IKT reaģēšanas un seku novēršanas plānus, ar mērķi nodrošināt tā funkciju saglabāšanu, savlaicīgu darbību atjaunošanu un *CCP* pienākumu izpildi.";

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

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

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

"3. Lai nodrošinātu konsekventu šā panta piemērošanu, EVTI izstrādā regulatīvo tehnisko standartu projektu, kurā precizē ziņas par 1. punktā minēto reģistrācijas pieteikumu, izņemot prasības saistībā ar IKT riska pārvaldību.";

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

"1. Darījumu reģistrs identificē darbības riska cēloņus un pēc iespējas samazina tos arī, izstrādājot atbilstošas sistēmas, kontroli un procedūras, tostarp IKT sistēmas, ko pārvalda saskaņā ar Regulu (ES) 2022/2554.

2. Darījumu reģistrs izveido, īsteno un uztur atbilstošu uzņēmējdarbības nepārtrauktības politiku un negadījuma seku novēršanas plānu, tostarp saskaņā ar Regulu (ES) 2022/2554 izveidotu IKT uzņēmējdarbības nepārtrauktības politiku un IKT reaģēšanas un seku novēršanas plānus, kā mērķis ir nodrošināt savu funkciju uzturēšanu, savlaicīgu darbības atsākšanu un darījumu reģistra pienākumu izpildi.";

5) regulas 80. panta 1. punktu svītro;

6) regulas I pielikuma II iedaļu groza šādi:

a) iedaļas a) un b) punktu aizstāj ar šādiem:

"a) darījumu reģistrs pārkāpj 79. panta 1. punktu, ja tas neatklāj darbības riska cēloņus vai nemēģina tos pēc iespējas samazināt, izstrādājot atbilstošas sistēmas, kontroli un procedūras, tostarp IKT sistēmas, ko pārvalda saskaņā ar Regulu (ES) 2022/2554;

b) darījumu reģistrs pārkāpj 79. panta 2. punktu, ja tas neizveido, neīsteno vai neuztur atbilstošu uzņēmējdarbības nepārtrauktības politiku un negadījuma seku novēršanas plānu, kurš ir izveidots saskaņā ar Regulu (ES) 2022/2554 ar mērķi nodrošināt tā funkciju uzturēšanu, savlaicīgu darbības atsākšanu un darījumu reģistra pienākumu izpildi;";

b) iedaļas c) punktu svītro;

7) regulas III pielikumu groza šādi:

a) pielikuma II iedaļu groza šādi:

i) iedaļas c) punktu aizstāj ar šādu:

"c) 2. līmeņa *CCP* pārkāpj 26. panta 3. punktu, ja tas neuztur vai neizmanto organizatorisko struktūru, kas nodrošina tā pakalpojumu un darbību veikšanas nepārtrauktību un pareizu funkcionēšanu, vai neizmanto piemērotas un samērīgas sistēmas, resursus vai procedūras, tostarp IKT sistēmas, ko pārvalda saskaņā ar Regulu (ES) 2022/2554;";

ii) iedaļas f) punktu svītro;

b) pielikuma III iedaļas a) punktu aizstāj ar šādu:

"a) 2. līmeņa *CCP* pārkāpj 34. panta 1. punktu, ja tas neizveido, neīsteno vai neuztur piemērotu uzņēmējdarbības nepārtrauktības politiku un negadījuma seku novēršanas plānu, kurš ir izveidots saskaņā ar Regulu (ES) 2022/2554 ar mērķi nodrošināt tā funkciju saglabāšanu, savlaicīgu darbību atjaunošanu un *CCP* pienākumu izpildi, kas vismaz ļauj atjaunot visus darījumus kopš pārtraukšanas brīža, lai *CCP* varētu turpināt droši darboties un pabeigt norēķinus paredzētajā dienā;".

61. 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 politiku, ko izveido un pārvalda saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2022/2554 (*), kā arī izmantojot jebkādus citus atbilstīgus rīkus, kontroli un procedūras attiecībā uz cita veida operacionālo risku, tostarp visām tā uzturētajām vērtspapīru norēķinu sistēmām.

_____

(*) Eiropas Parlamenta un Padomes Regula (ES) 2022/2554 (2022. gada 14. decembris) par finanšu sektora digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011 (OV L 333, 27.12.2022, 1.. 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, tostarp saskaņā ar Regulu (ES) 2022/2554 izveidotu IKT uzņēmējdarbības nepārtrauktības nodrošināšanas politiku un IKT reaģēšanas un 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) 2022/2554 12. panta 5. un 7. punktā.";

4) panta 6. punktu aizstāj ar šādu:

"6. 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:

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

62. 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 aizstāj ar šādu:

"4. APS ievēro tīklu un informācijas sistēmu drošības prasības, kas noteiktas Eiropas Parlamenta un Padomes Regulā (ES) 2022/2554 (*).

(*) Eiropas Parlamenta un Padomes Regula (ES) 2022/2554 (2022. gada 14. decembris) par finanšu sektora digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011 (OV L 333, , 27.12.2022., 1.. lpp.).";

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

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

2) regulas 27.h pantu groza šādi:

a) panta 5. punktu aizstāj ar šādu:

"5. KDLN ievēro tīklu un informācijas sistēmu drošības prasības, kas noteiktas Regulā (ES) 2022/2554.";

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

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

3) regulas 27.i pantu groza šādi:

a) panta 3. punktu aizstāj ar šādu:

"3. AZS ievēro tīklu un informācijas sistēmu drošības prasības, kas noteiktas Regulā (ES) 2022/2554.";

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

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

63. pants

Grozījumi Regulā (ES) 2016/1011

Regulas (ES) 2016/1011 6. pantam pievieno šādu punktu:

"6. Attiecībā uz kritiski svarīgiem etaloniem administratoram 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) 2022/2554 (*).

(*) Eiropas Parlamenta un Padomes Regula (ES) 2022/2554 (2022. gada 14. decembris) par finanšu sektora digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011 (OV L 333, 27.12.2022, 1.. lpp.)."

64. pants

Stāšanās spēkā un piemērošana

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

To piemēro no 2025. gada 17. janvāra.

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

Strasbūrā, 2022. gada 14. decembrī

Eiropas Parlamenta vārdā –	*Padomes vārdā –*
priekšsēdētāja	*priekšsēdētājs*
R. METSOLA	M. BEK